H.R. 4435—FY15 NATIONAL DEFENSE AUTHORIZATION BILL

SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS AND CAPABILITIES

SUMMARY OF BILL LANGUAGE

Table Of Contents

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE I—PROCUREMENT

LEGISLATIVE PROVISIONS

SUBTITLE C—NAVY PROGRAMS

Section 123—Additional Oversight Requirements for the Undersea Mobility Acquisition Program of the United States Special Operations Command

This section would modify the current oversight requirements for the undersea mobility acquisition program of U.S. Special Operations Command, and require the Secretary of the Navy to review a transition plan for the undersea mobility capabilities developed by the Commander, U.S. Special Operations Command. This section would also repeal section 144 of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112-81).

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

LEGISLATIVE PROVISIONS

SUBTITLE B—PROGRAM REQUIREMENTS, RESTRICTIONS, AND LIMITATIONS

Section 214—Limitation on Availability of Funds for Airborne Reconnaissance Systems

This section would limit the obligation or expenditure of funds to not more than 25 percent for the imaging and targeting support of airborne reconnaissance systems, until the Secretary of the Air Force delivers a report to the congressional defense committees and the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate. The elements of the report would include a detailed plan regarding using such funds for fiscal year 2015, and a strategic plan for the funding of advanced airborne reconnaissance technologies supporting manned and unmanned systems.

The committee notes that the Air Force did not provide substantive information for the proposed use of these funds, aside from the general area of imaging and targeting support.

SUBTITLE C—OTHER MATTERS

Section 221—Revision to the Service Requirement under the Science, Mathematics, and Research for Transformation Defense Education Program

This section would amend subparagraph (B) of section 2192a(c)(1) of title 10, United States Code, by modifying the service obligation requirement to also include employment with a public or private sector entity or organization outside the Department of Defense if the Secretary of Defense determines that employment of the person with such entity or organization for the purpose of such obligated service would provide a benefit to the Department of Defense.

Section 222—Modification to Cost-sharing Requirement for Pilot Program to include Technology Protection Features during Research and Development of Certain Defense Systems

This section would amend Section 243(b) of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111-383) by striking "at least one half of the cost of such activities" and inserting "an appropriate share of the cost of such activities, as determined by the Secretary".

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

LEGISLATIVE PROVISIONS

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

Section 802—Extension of Contract Authority for Advanced Component Development or Prototype Units

This section would extend existing statutory authority under subsection (b)(4) of section 819 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111-84; 10 U.S.C. 2302 note) until September 30, 2019. This authority provides the Department of Defense a "bridge" between the science and technology portion of a contract awarded under the Federal Acquisition Regulation's Broad Agency Announcement authority, and the award of a contract under a new acquisition for advanced component development or production.

TITLE X—GENERAL PROVISIONS

LEGISLATIVE PROVISIONS

SUBTITLE D—COUNTERTERRORISM

Section 1031—Extension of Authority to Make Rewards for Combating Terrorism

This section would extend the authority through fiscal year 2015 for the Secretary of Defense to offer and make rewards to a person providing information or nonlethal assistance to U.S. Government personnel or Government personnel of allied forces participating in a combined operation with U.S. Armed Forces conducted outside the United States against international terrorism or providing such information or assistance that is beneficial to force protection associated with such an operation.

SUBTITLE E—MISCELLANEOUS AUTHORITIES AND LIMITATIONS

Section 1041—Modification of Department of Defense Authority for Humanitarian Demining Assistance and Stockpiled Conventional Munitions Assistance Programs

This section would modify the reporting requirements and definitions contained in section 407 of title 10, United States Code, regarding humanitarian demining assistance and stockpiled conventional munitions assistance. The committee is also concerned that the Department of Defense Humanitarian Mine Action (HMA) program have sufficient resources for HMA and conventional munitions assistance programs.

Section 1045—Certification and Limitation on Availability of Funds for Aviation Foreign Internal Defense Program

This section would prohibit U.S. Special Operations Command from obligating any funds available for fiscal year 2015 for the Aviation Foreign Internal Defense Program until the Secretary of Defense provides a certification to the congressional defense committees that validates program requirements.

SUBTITLE F—STUDIES AND REPORTS

Section 1051—Protection of Defense Mission-Critical Infrastructure from Electromagnetic Pulse and High-Powered Microwave Systems

This section would require the Secretary of Defense to submit a certification to the congressional defense committees that defense mission-critical infrastructure requiring electromagnetic pulse protection that receives power supply from commercial or other non-military sources, is protected from the adverse effects of man-made or naturally occurring electromagnetic pulse and high-powered microwave weapons.

The committee is aware that the Department of Defense is dependent on commercial power to supply most of its needs and understands that such commercial power could be susceptible to disruption or degradation from electromagnetic pulse or high-powered microwave events. The committee believes that much of the Department's defense mission-critical infrastructure includes planning and mitigation measures against such threats, but remains concerned that some critical capabilities may not have been included in previous reviews. The committee intends to determine if there is reason for further concern, but recognizes that remediation activities will have to be resourced by other organizations outside of the Department of Defense.

SUBTITLE G—OTHER MATTERS

Section 1062—Reduction in Costs to Report Critical Changes to Major Automated Information System Programs

This section would give Department of Defense milestone decision authorities responsible for major automated information system programs or major information technology investments the option of submitting a notification to the congressional defense committees, either a critical change report when required, or a streamlined notification when the official concludes that the critical change occurred due to an extension of the program and there is minimal developmental risk.

Section 1064—Pilot Program for the Human Terrain System

This section would require the Secretary of the Army to conduct a pilot program to utilize Human Terrain System assets in the U.S. Pacific Command area of responsibility to support Phase 0 shaping operations and to support the theater security cooperation plans of the geographic combatant commander.

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

LEGISLATIVE PROVISIONS

SUBTITLE D—OTHER MATTERS

Section 1231—Extension of Authority for Support of Special Operations to Combat Terrorism

This section would extend through 2017 the authority for support of special operations to combat terrorism pursuant to section 1208 of the Ronald Reagan National Defense Authorization Act for Fiscal Year 2005 (Public Law 108-375), as amended most recently by section 1203(c) of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112-81). Further discussion of this provision is contained in the classified annex to this report.

Section 1232—One-Year Extension of Authorization for Non-Conventional Assisted Recovery Capabilities

This section would extend by 1 year the authority for non-conventional assisted recovery capabilities pursuant to subsection (h) of section 943 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110-417), as amended most recently by section 1203(c) of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112-81).

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE B—DEFENSE INTELLIGENCE AND INTELLIGENCE-RELATED ACTIVITIES

Section 1611—Assessment and Limitation on Availability of Funds for Intelligence Activities and Programs of United States Special Operations Command and Special Operations Forces

This section would require the Secretary of Defense, acting through the Under Secretary of Defense for Intelligence, the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, and the Director of the Defense

Intelligence Agency, to submit an assessment to the appropriate congressional committees on the intelligence activities and programs of the U.S. Special Operations Forces and U.S. Special Operations Command. This section would also limit 50 percent of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2015 of U.S. Special Operations Command Major Force Program-11 procurement, defense-wide, and research, development, testing, and evaluation, defense-wide, until such assessment is received. Further discussion of this provision is contained in the classified annex to this report.

Section 1612—Annual Briefing on the Intelligence, Surveillance, and Reconnaissance Requirements of the Combatant Commands

This section would direct the Chairman of the Joint Chiefs of Staff to provide a briefing to the congressional defense committees and the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate on the intelligence, surveillance, and reconnaissance requirements, by specific intelligence capability type, of each of the combatant commands; for the year preceding the year in which the briefing is provided, the satisfaction rate of each of the combatant commands with the intelligence, surveillance, and reconnaissance requirements, by specific intelligence capability type, of such combatant command; and a risk analysis identifying the critical gaps and shortfalls in such requirements in relation to such satisfaction rate.

Additionally, the Under Secretary of Defense for Intelligence would be required to provide a briefing to the congressional defense committees and the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate on short-term, mid-term, and long-term strategies to address the critical intelligence, surveillance, and reconnaissance requirements of the combatant commands. The briefings should address the role of government and commercial systems, and the methods to meeting the requirements of the combatant commands.

These briefings would be due with the budget submission each year, from fiscal year 2016-20.

Section 1613—One-Year Extension of Report on Imagery Intelligence and Geospatial Information Support Provided to Regional Organizations and Security Alliances

This section would extend the existing reporting requirement by 1 year, regarding sharing of imagery intelligence and geospatial information to regional organizations and security alliances.

Section 1614—Tactical Exploitation of National Capabilities Executive Agent

This section would establish an executive agent for the Tactical Exploitation of National Capabilities (TENCAP) program. The executive agent shall report directly to the Under Secretary of Defense for Intelligence, and shall be responsible for working with the combatant commands, military services, and intelligence community to develop methods to increase warfighter effectiveness through the exploitation of national capabilities and to promote cross-domain integration of such capabilities into military operations, training, intelligence, surveillance, and reconnaissance activities.

This section would also require the TENCAP executive agent to provide an annual briefing to the Committees on Armed Services of the Senate and the House of Representatives and the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives for the fiscal years 2016-20 on the investments, activities, challenges, and opportunities in carrying out the TENCAP program.

SUBTITLE C—CYBERSPACE-RELATED MATTERS

Section 1621—Executive Agency for Cyber Test and Training Ranges

This section would require the Secretary of Defense to establish an executive agent to coordinate and oversee the management of the various cyber test and training ranges being developed and deployed by the Department of Defense.

The committee is aware that a number of cyber ranges currently exist, but the Department's Test and Evaluation Strategic Plan has identified a number of capability gaps that need to be addressed in order to provide sufficient and adequate cyber test and training. Though there has been significant growth of cyber personnel to fulfill critical defensive and offensive missions for the Department, the capacity for training in a realistic environment has not kept pace. The committee is concerned that those challenges have not been addressed and that the Department is unable to come to resolution on how best to provide adequate management and support for such capabilities. The committee believes that designation of an executive agent for cyber test and training ranges will be an important step in managing the current range resources, as well as provide discipline to prevent rampant proliferation of duplicative capabilities.

BILL LANGUAGE

SEC. 123.[Log 53920] ADDITIONAL OVERSIGHT REQUIREMENTS FOR THE UNDERSEA MOBILITY ACQUISITION PROGRAM OF THE UNITED STATES SPECIAL OPERATIONS COMMAND.

(a) LIMITATION ON MILESTONE B DECISION.—The Commander of the United States Special Operations Command may not make any Milestone B acquisition decisions with respect to a covered element unless—

(1) the Commander has submitted to the congressional defense committees the transition plan under subsection (b)(2);

(2) the Under Secretary of Defense for Acquisition, Technology, and Logistics has submitted to such committees the certification under subsection (c)(1); and

(3) the Secretary of the Navy has completed the review under subsection (d)(1).

(b) TRANSITION PLAN.—

(1) IN GENERAL.—The Commander shall develop a transition plan for undersea mobility capabilities that includes the following:

(A) A description of the current capabilities provided by covered elements as of the date of the plan.

SEC. 214.[Log 53759] LIMITATION ON AVAILABILITY OF FUNDS FOR AIRBORNE RECONNAISSANCE SYSTEMS.

(a) LIMITATION.—Of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2015 for research, development, test, and evaluation, Air Force, for imaging and targeting support of airborne reconnaissance systems, not more than 25 percent may be obligated or expended until the date on which the Secretary of the Air Force submits to the appropriate congressional committees—

(1) a detailed plan regarding using such funds for such purpose during fiscal year 2015; and

(2) a strategic plan for the funding of advanced airborne reconnaissance technologies supporting manned and unmanned systems.

(b) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means—

(1) the congressional defense committees; and

(2) the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

Subtitle C—Other Matters

SEC. 221. [Log 53651] REVISION TO THE SERVICE REQUIREMENT UNDER THE SCIENCE, MATHEMATICS, AND RESEARCH FOR TRANSFORMATION DEFENSE EDUCATION PROGRAM.

Subparagraph (B) of section 2192a(c)(1) of title 10, United States Code, is amended to read as follows:

''(B) in the case of a person not an employee of the Department of Defense, the person shall enter into a written agreement to accept and continue employment for the period of obligated service determined under paragraph (2)—

''(i) with the Department of Defense; or

''(ii) with a public or private entity or organization outside the Department if the Secretary of Defense determines that employment of the person with such entity or organization for the purpose of such obligated service would provide a benefit to the Department.''.

SEC. 222.[Log 53650] MODIFICATION TO COST-SHARING REQUIREMENT FOR PILOT PROGRAM TO INCLUDE TECHNOLOGY PROTECTION FEATURES DURING RESEARCH AND DEVELOPMENT OF CERTAIN DEFENSE SYSTEMS.

Section 243(b) of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (10 U.S.C. 2358 note) is amended in the matter following paragraph (2) by striking ''at least one-half of the cost of such activities'' and inserting ''an appropriate share of the cost of such activities, as determined by the Secretary''.

SEC. 802 [Log 53717]. EXTENSION OF CONTRACT AUTHORITY FOR ADVANCED COMPONENT DEVELOPMENT OR PROTOTYPE UNITS.

(a) EXTENSION OF TERMINATION.—Subsection (b)(4) of section 819 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84; 10 U.S.C. 2302 note) is amended by striking ''September 30, 2014'' and inserting ''September 30, 2019''.

(b) EXTENSION OF REPORT REQUIREMENT.—Subsection (c) of such section is amended by striking ''March 1, 2013'' and inserting '' March 1, 2018''.

Subtitle D—Counterterrorism

SEC. 1031 [Log53200]. EXTENSION OF AUTHORITY TO MAKE REWARDS FOR COMBATING TERRORISM.

Section 127b(c)(3)(C) of title 10, United States Code, is amended by striking ''September 30, 2014'' and inserting ''September 30, 2015''.

Subtitle E—Miscellaneous Authorities and Limitations

SEC. 1041 [Log 53826]. MODIFICATION OF DEPARTMENT OF DEFENSE AUTHORITY FOR HUMANITARIAN DEMINING ASSISTANCE AND STOCKPILED CONVENTIONAL MUNITIONS ASSISTANCE PROGRAMS.

(a) INCLUSION OF INFORMATION ABOUT INSUFFICIENT FUNDING IN ANNUAL REPORT.—Subsection (d)(3) of section 407 of title 10, United States Code, is amended by inserting ''or insufficient funding'' after ''such activities'';

(b) DEFINITION OF STOCKPILED CONVENTIONAL MUNITIONS ASSISTANCE.—Subsection (e)(2) of such section is amended—

(1) by striking ''and includes'' and inserting the following: ''small arms, and light weapons, including man-portable air-defense systems. Such term includes''; and

(2) by inserting before the period at the end the following: '', small arms, and light weapons, including man-portable air-defense systems''.

SEC. 1045 [Log 53749]. CERTIFICATION AND LIMITATION ON AVAILABILITY OF FUNDS FOR AVIATION FOREIGN INTERNAL DEFENSE PROGRAM.

(a) CERTIFICATION.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a certification regarding the aviation foreign internal defense program that includes each of the following:

(A) An overall description of the program, included validated requirements from each of the geographic combatant commands and the Joint Staff, and statutory authorities used to support fixed and rotary wing aviation foreign internal defense programs within the Department of Defense.

(B) Program goals, proposed metrics of performance success, and anticipated procurement and operation and maintenance costs across the Future Years Defense Program.

(C) A comprehensive strategy outlining and justifying contributing commands and units for program execution, including the use of Air Force, Special Operations Command, Reserve, and National Guard forces and components.

(D) The results of any analysis of alternatives and efficiencies reviews for any contracts awarded to support the aviation foreign internal defense program.

(E) Any other items the Secretary of Defense determines appropriate.

(2) FORM.—The certification required under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(b) LIMITATIONS.—

(1) LIMITATIONS ON THE USE OF FUNDS.—None of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2015 may be obligated or expended to support the aviation foreign internal defense program, or to retire, transfer, or divest any asset of such program, until the date that is 45 days after the date on which the Secretary of Defense provides to the congressional defense committees the certification required under subsection (a).

(2) LIMITATION ON DISPOSITION OF AIRCRAFT.—No aircraft that, as of the date of the enactment of this Act, is part of the aviation foreign internal defense program may be transferred into or maintained in a status that is considered excess to

the requirements of the possessing command and awaiting disposition instructions.

Subtitle F—Studies and Reports

SEC. 1051 [Log 53868]. PROTECTION OF DEFENSE MISSION-CRITICAL INFRASTRUCTURE FROM ELECTROMAGNETIC PULSE AND HIGH-POWERED MICROWAVE SYSTEMS.

(a) CERTIFICATION REQUIRED.—Not later than June 1, 2015, the Secretary of Defense shall submit to the congressional defense committees certification that defense mission-critical infrastructure requiring electromagnetic pulse protection that receives power supply from commercial or other non-military sources is protected from the adverse effects of man-made or naturally occurring electromagnetic pulse and high-powered microwave weapons.

(b) FORM OF SUBMISSION.—The certification required by subsection (a) shall be submitted in classified form.

(c) DEFINITIONS.—In this section:

(1) The term ''defense mission-critical infrastructure'' means Department of Defense infrastructure of defense critical systems essential to project, support, and sustain the Armed Forces and military operations worldwide.

(2) The term ''defense critical system'' means a primary mission system or an auxiliary or supporting system—

(A) the operational effectiveness and operational suitability of which are essential to the successful mission completion or to aggregate residual combat capability; and

(B) the failure of which would likely result in the failure to complete a mission.

SEC. 1062 [Log 53204]. REDUCTION IN COSTS TO REPORT CRITICAL CHANGES TO MAJOR AUTOMATED INFORMATION SYSTEM PROGRAMS.

(a) EXTENSION OF A PROGRAM DEFINED.—Section 2445a of title 10, United States Code, is amended adding at the end the following new subsection:

''(g) EXTENSION OF A PROGRAM.—In this chapter, the term 'extension of a program' means, with respect to a major automated information system program or other major information technology investment program, the further deployment or planned deployment to additional users of the system which has already been found operationally effective and suitable by an independent test agency or the Director of Operational Test and Evaluation, beyond the scope planned in the original estimate or information originally submitted on the program.''.

(b) REPORTS ON CRITICAL CHANGES IN MAIS PROGRAMS.—Subsection (d) of section 2445c of such title is amended—

(1) in paragraph (1), by striking ''paragraph (2)'' and inserting ''paragraph (3)'';

(2) by redesignating paragraph (2) as paragraph (3); and

(3) by inserting after paragraph (1) the following new paragraph (2):

''(2) NOTIFICATION WHEN VARIANCE DUE TO EXTENSION OF PROGRAM.—If the milestone decision authority for a program who, following receipt of a quarterly report described in paragraph (1) and making a determination described in paragraph (3), also determines that the circumstances resulting in the determination described in paragraph (3) are primarily due to an extension of a program, the official may, in lieu of carrying out an evaluation and submitting a report in accordance with paragraph (1), submit to the congressional defense committees, within 45 days after receiving the quarterly report, a notification that the official has made such determinations and a certification that such determinations involve minimal developmental risk. If such a notification is submitted, the limitation in subsection (g)(1) does not apply with respect to that determination under paragraph (3).''.

(c) CONFORMING CROSS-REFERENCE AMENDMENT.—Subsection (g)(1) of such section is amended by striking ''subsection (d)(2)'' and inserting ''subsection (d)(3)''.

(d) TOTAL ACQUISITION COST INFORMATION.—Title 10, United States Code, is further amended—

(1) in section 2445b(b)(3), by striking ''development costs'' and inserting ''total acquisition costs''; and

(2) in section 2445c—

(A) in subparagraph (B) of subsection (c)(2), by striking ''program development cost'' and inserting ''total acquisition cost''; and

(B) in subparagraph (C) of subsection (d)(3) (as redesignated by subsection (b)(2)), by striking ''program development cost'' and inserting ''total acquisition cost''.

(e) CLARIFICATION OF CROSS-REFERENCE.—Section 2445c(g)(2) of such title is amended by striking ''in compliance with the requirements of subsection (d)(2)'' and inserting ''under subsection (d)(1)(B)''.

SEC. 1064 [Log 53164]. PILOT PROGRAM FOR THE HUMAN TERRAIN SYSTEM.

(a) PILOT PROGRAM REQUIRED.—The Secretary of the Army shall carry out a pilot program under which the Secretary uses the Human Terrain System assets in the Pacific Command area of responsibility to support phase 0 shaping operations and the theater security cooperation plans of the Commander of the Pacific Command.

(b) LIMITATION.—Not more than 12 full-time equivalent personnel, or 12 full-time equivalent personnel for reach back support, may be deployed into the Pacific command area of responsibility to support the pilot program required by subsection (a). The limitation under the preceding sentence shall not apply to training or support functions required to prepare personnel for participation in the pilot program.

(c) REPORTS.—

(1) BRIEFING.—Not later than 60 days after the date of the enactment of this Act, the Secretary of the Army shall provide to the congressional defense committees a briefing on the plan of the Secretary to carry out the program required by subsection (a), including the milestones, metrics, deliverables, and resources needed to execute such a pilot program. In establishing the metrics for the pilot program, the Secretary shall include the ability

to measure the value of the program in comparison to other analytic tools and techniques.

(2) INITIAL REPORT.—Not later than one year after the date of the enactment of this Act, the Secretary of the Army shall submit to the congressional defense committees a report on the status of the pilot program. Such report shall include the independent analysis and recommendations of the Commander of the Pacific Command regarding the effectiveness of the program and how it could be improved.

(3) FINAL REPORT.—Not later than December 1, 2016, the Secretary of the Army shall submit to the congressional defense committees a final report on the pilot program. Such report shall include an analysis of the comparative value of human terrain information relative to other analytic tools and techniques, recommendations regarding expanding the program to include other combatant commands, and any improvements to the program and necessary resources that would enable such an expansion.

(d) TERMINATION.—The authority to carry out a pilot program under this section shall terminate on September 30, 2016.

Subtitle D—Other Matters

SEC. 1231. [LOG 53193] EXTENSION OF AUTHORITY FOR SUPPORT OF SPECIAL OPERATIONS TO COMBAT TERRORISM.

Section 1208(h) of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (Public Law 108–375; 118 Stat. 2086), as most recently amended by section 1203(c) of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112–81; 125 Stat. 1621), is further amended by striking ''2015'' and inserting ''2017''.

SEC. 1232. [LOG 53908] ONE-YEAR EXTENSION OF AUTHORIZATION FOR NON-CONVENTIONAL ASSISTED RECOVERY CAPABILITIES.

(a) EXTENSION.—Subsection (h) of section 943 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110–417; 122 Stat. 4579), as most recently amended by section 1241 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66; 127 Stat. 920), is further amended by striking ''2015'' and inserting ''2016''.

(b) CROSS-REFERENCE AMENDMENT.—Subsection (f) of such section is amended by striking ''413b(e)'' and inserting ''3093(e)''.

Subtitle B—Defense Intelligence and Intelligence-Related Activities

SEC. 1611 [Log 53199]. ASSESSMENT AND LIMITATION ON AVAILABILITY OF FUNDS FOR INTELLIGENCE ACTIVITIES AND PROGRAMS OF UNITED STATES SPECIAL OPERATIONS COMMAND AND SPECIAL OPERATIONS FORCES.

(a) ASSESSMENT.—

(1) REQUIREMENT.—The Secretary of Defense, acting through the Under Secretary of Defense for Intelligence, the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, and the Director of the Defense Intelligence Agency, shall submit to the appropriate committees of Congress an assessment of the intelligence activities and programs of United States Special Operations Command and special operations forces.

(2) INCLUSIONS.—The assessment under paragraph (1) shall include each of the following elements:

(A) An overall strategy defining such intelligence activities and programs, including definitions of intelligence activities and programs unique to special operations.

(B) A validated strategy and roadmap of intelligence, surveillance, and reconnaissance programs and requirements for special operations across the future years defense program.

(C) A comprehensive description of current and anticipated future Joint Staff validated requirements for the intelligence activities and programs of each geographic combatant commander within the respective geographic area of such covered combatant commander to be fulfilled by special operations forces, including those that can only be addressed by special operations forces, programs, or capabilities.

(D) Validated present and planned United States Special Operations Command force structure requirements to meet current and anticipated special operations intelligence activities and programs of geographic combatant commanders.

(E) A comprehensive review and assessment of statutory authorities, and Department and interagency policies, including limitations, for special operations forces intelligence activities and programs.

(F) An independent, comprehensive cost estimate of special operations intelligence activities and programs by the Director of Cost Assessment and Program Evaluation of the Department of Defense, including an estimate of the costs of the period of the current future years defense program, including a description of all rules and assumptions used to develop the cost estimates.

(G) A copy of any memoranda of understanding or memoranda of agreement between the Department of Defense and other departments or agencies of the United States Government, or between components of the Department of Defense that are required to implement objectives of special operations intelligence activities and programs.

(H) Any other matters the Secretary considers appropriate.

(3) FORM.—The assessment required under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(b) LIMITATIONS.—

(1) IN GENERAL.—Subject to paragraph (2), not more than 50 percent of the funds authorized to

be appropriated by this Act or otherwise made available for fiscal year 2015 for procurement, Defense-wide, or research, development, test, and evaluation, Defense-wide, for the major force program 11 of the United States Special Operations Command may be obligated until the assessment required under subsection (a) is submitted.

(2) EXCEPTION.—Paragraph (1) shall not apply with respect to funds authorized to be appropriated for Overseas Contingency Operations under title XV.

(c) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of congress'' means the congressional defense committees, the Permanent Select Committee on Intelligence of the House of Representatives, and the Select Committee on Intelligence of the Senate.

(2) FUTURE YEARS DEFENSE PROGRAM.—The term ''future years defense program'' means the future years defense program under section 221 of title 10, United States Code.

(3) GEOGRAPHIC COMBATANT COMMANDER.—The term ''geographic combatant commander'' means a commander of a combatant command (as

defined in section 161(c) of title 10, United States Code) with a geographic area of responsibility.

SEC. 1612 [Log 53213]. ANNUAL BRIEFING ON THE INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE REQUIREMENTS OF THE COMBATANT COMMANDS.

At the same time that the President's budget is submitted pursuant to section 1105(a) of title 31, United States Code, for each of fiscal years 2016 through 2020—

(1) the Chairman of the Joint Chiefs of Staff shall provide to the congressional defense committees, the Permanent Select Committee on Intelligence of the House of Representatives, and the Select Committee on Intelligence of the Senate a briefing on—

(A) the intelligence, surveillance, and reconnaissance requirements, by specific intelligence capability type, of each of the combatant commands;

(B) for the year preceding the year in which the briefing is provided, the satisfaction rate of each of the combatant commands with the intelligence, surveillance, and reconnaissance requirements, by specific intelligence capability type, of such combatant command; and

(C) a risk analysis identifying the critical gaps and shortfalls in such requirements in relation to such satisfaction rate; and

(2) the Under Secretary of Defense for Intelligence shall provide to the congressional defense committees, the Permanent Select Committee on Intelligence of the House of Representatives, and the Select Committee on Intelligence of the Senate a briefing on short-term, mid-term, and long-term strategies to address the critical intelligence, surveillance and reconnaissance requirements of the combatant commands.

SEC. 1613 [Log 53214]. ONE-YEAR EXTENSION OF REPORT ON IMAGERY INTELLIGENCE AND GEOSPATIAL INFORMATION SUPPORT PROVIDED TO REGIONAL ORGANIZATIONS AND SECURITY ALLIANCES.

Section 921(c)(1) of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239; 126 Stat. 1878) is amended by striking ''2014 and 2015'' and inserting ''2014 through 2016''.

SEC. 1614 [Log 53215]. TACTICAL EXPLOITATION OF NATIONAL CAPABILITIES EXECUTIVE AGENT.

Subchapter I of chapter 21 of title 10, United States Code, is amended by adding at the end the following new section:

"§ 430. TENCAP executive agent

''(a) IN GENERAL.—There is in the Department of Defense a Tactical Exploitation of National Capabilities Executive Agent who shall be appointed by the Under Secretary of Defense for Intelligence. The Executive Agent shall report directly to the Under Secretary of Defense for Intelligence. The Executive Agent shall be responsible for working with the combatant commands, military services, and the intelligence community to develop methods to increase warfighter effectiveness through the exploitation of national capabilities and to promote cross-domain integration of such capabilities into military operations, training, intelligence, surveillance, and reconnaissance activities.

''(b) ANNUAL BRIEFING.—At the same time as the budget materials are submitted to Congress in connection with the submission of the budget for each of fiscal years 2016 through 2020, pursuant to section 1105 of title 31, the Executive Agent, in coordination with the commanders of the combatant commands, the Secretaries of the military departments, and the heads of the Department of De-

fense intelligence agencies and offices, shall provide to the Committee on Armed Services and the Select Committee on Intelligence of the Senate and the Committee on Armed Services and the Permanent Select Committee on Intelligence of the House of Representatives a briefing on the investments, activities, challenges, and opportunities of the Executive Agent in carrying out the responsibilities under paragraph (1). The briefings shall be coordinated with each of the armed services, the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, and the National Reconnaissance office.''.

Subtitle C—Cyberspace-Related Matters

SEC. 1621 [Log 53586]. EXECUTIVE AGENCY FOR CYBER TEST AND TRAINING RANGES.

(a) EXECUTIVE AGENT.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Defense shall designate a senior official of the Department of Defense to act as the executive agent for cyber and information technology test and training ranges.

(b) ROLES, RESPONSIBILITIES, AND AUTHORITIES.—

(1) ESTABLISHMENT.—Not later than one year after the enactment of this Act, and in accordance with Directive 5101.1, the Secretary of Defense shall prescribe the roles, responsibilities, and authorities of the executive agent designated under subsection (a).

(2) SPECIFICATION.—The roles and responsibilities of the executive agent designated under subsection (a) shall include each of the following:

(A) Developing and maintaining a comprehensive list of cyber and information technology ranges, test facilities, test beds, and other means of testing, training, and developing

software, personnel, and tools for accommodating the mission of the Department.

(B) Serving as a single entity to organize and manage designated cyber and information technology test ranges, including—

(i) establishing the priorities for cyber and information technology ranges to meet Department objectives;

(ii) enforcing standards to meet requirements specified by the United States Cyber Command, the training community, and the research, development, testing, and evaluation community;

(iii) identifying and offering guidance on the opportunities for integration amongst the designated cyber and information technology ranges regarding test, training, and development functions;

(iv) finding opportunities for cost reduction, integration, and coordination improvements for the appropriate cyber and information technology ranges;

(v) adding or consolidating cyber and information technology ranges in the future to better meet the evolving needs of

the cyber strategy and resource requirements of the Department; and

(vi) coordinating with interagency and industry partners on cyber and information technology range issues.

(C) Defining a cyber range architecture that—

(i) may add or consolidate cyber and information technology ranges in the future to better meet the evolving needs of the cyber strategy and resource requirements of the Department;

(ii) coordinates with interagency and industry partners on cyber and information technology range issues;

(iii) allows for integrated closed loop testing in a secure environment of cyber and electronic warfare capabilities;

(iv) supports science and technology development, experimentation, testing and training; and

(v) provides for interconnection with other existing cyber ranges and other kinetic range facilities in a distributed manner.

(D) Certifying all cyber range investments of the Department of Defense.

(E) Performing such other roles and responsibilities as the Secretary of Defense considers appropriate.

(c) SUPPORT WITHIN DEPARTMENT OF DEFENSE.—In accordance with Directive 5101.1, the Secretary of Defense shall ensure that the military departments, Defense Agencies, and other components of the Department of Defense provide the executive agent designated under subsection (a) with the appropriate support and resources needed to perform the roles, responsibilities, and authorities of the executive agent.

(d) DEFINITIONS.—In this section:

(1) The term ''designated cyber and information technology range'' includes the National Cyber Range, the Joint Information Operations Range, the Defense Information Assurance Range, and the C4 Assessments Division of J6 of the Joint Staff.

(2) The term ''Directive 5101.1'' means Department of Directive 5101.1, or any successor directive relating to the responsibilities of an executive agent of the Department of Defense.

(3) The term ''executive agent'' has the meaning given the term ''DoD Executive Agent'' in Directive 5101.1.

DIRECTIVE REPORT LANGUAGE

Table Of Contents

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE I—PROCUREMENT

OTHER PROCUREMENT, ARMY

Items of Special Interest

Personal dosimetry for protection in Chemical Biological Radiological Nuclear and Explosive environments

The committee remains concerned about the increasing proliferation of Chemical Biological Radiological Nuclear and Explosive (CBRNE) Weapons of Mass Destruction, and believes that maintaining adequate modern protective equipment is of critical importance for the safety of U.S. forces in CBRNE environments. The committee notes that in regard to radiological hazards, accurate dosimetry is critical to the forecast of type, severity, and expected time of onset of symptoms, information needed to predict a person's fitness for duty, and the provision of combat readiness information. The committee notes that the Department of the Army last validated a requirement for Individual Personal Dosimeters in 1975. However, the nuclear and radiological threat environment facing the Joint Force has changed dramatically over the past four decades and dosimeter technology has also improved. The committee is aware of efforts within the Department of Defense to develop a Joint Personal Dosimeter (JPD) and validate an updated requirement for the JPD. The committee understands that the JPD is expected to enter miestone C late in fiscal year 2015. The committee is concerned, however, that procuring JPDs to replace legacy Army systems will not begin until 2020, at the earliest. In addition, the committee notes that the Army currently has nearly 8,500 legacy systems programmed for replacement.

Therefore, the committee encourages the Army to begin JPD procurement to replace legacy Army systems as soon after the milestone C decision as the availability of funds will allow. Furthermore, the committee directs the Secretary of Defense to provide a briefing to the committee by September 1, 2014, on the status of the JPD program and the efforts to validate an updated dosimetry requirement for the JPD. The briefing should include any recommendations that the Secretary has to begin procurement of JPDs earlier than 2020.

OTHER PROCUREMENT, AIR FORCE

Items of Special Interest

Beyond line of sight command and control for intelligence, surveillance, and reconnaissance systems

The committee is encouraged by the advances in distribution of full motion video and the bridging of disparate radio wave forms for enhanced interoperability

as part of the Joint Aerial Layered Network. The committee recognizes that the fielding of beyond line of sight command and control and associated tactical pods in support of intelligence, surveillance, and reconnaissance will provide valuable capabilities in response to stated urgent combatant commander requirements.

Yet, the committee is concerned that a joint capability, called Tactical Airborne Communications Pod (TACPod) was developed using Air Force Quick Reaction Capability funding and processes, but is not being used across the military services. Rather than deploying the capability to meet combatant commander validated requirements, TACPod is instead being stored indefinitely. Separately, the committee is concerned that the Air Force is procuring an entirely different capability to meet essentially the same requirements that TACPod was originally developed to fulfill.

Therefore, the committee directs the Secretary of the Air Force, in coordination with the Secretary of the Navy and the Under Secretary of Defense for Acquisition, Technology, and Logistics, to provide a briefing to the committee by November 1, 2014, on the existing and planned activities in support of beyond line of sight command and control for intelligence, surveillance, and reconnaissance systems.

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, ARMY

Items of Special Interest

High Performance Computing Modernization program

The committee is aware that the Army Corps of Engineers serves as executive agent for the Department of Defense High Performance Computing Modernization (HPCM) program, a responsibility that devolved from the Office of the Secretary of Defense in fiscal year 2012. The purpose of this program is to apply supercomputing resources to solve Department of Defense problems in research, development, test, and evaluation, and acquisition engineering. To meet this mission, the HPCM program must maintain state-of-the-art supercomputing resource centers, as well as software engineering talent to maintain modern and secure software applications for the user community.

The committee is also aware that the HPCM program has been operating at a level not currently supported by the level of funding requested in the President's request. The committee is concerned that the shortfall has only been mitigated by the repeated intervention of Congress to get the program to a sustainable level. The committee believes that the Department should conduct a thorough assessment of the program to ensure future budget requests are sufficient to right-size the budget to the needed infrastructure and support capabilities.

Therefore, the committee directs the Secretary of the Army, in coordination with the Assistant Secretary of Defense for Research and Engineering, to review the HPCM program, and to submit a report on the findings to the congressional defense committees not later than September 30, 2014. The review should examine the following:

(1) Identify the capabilities that will be lost and the impact on Department if the HPCMP is funded at the budget request for fiscal year 2015 level throughout the Future Years Defense Program (FYDP);

(2) Identify the resources reduced, including manpower, in order to operate at the budget request for fiscal year 2015 level throughout the FYDP; and

(3) A strategy for closing the gap between the budget requests and the fiscal year 2012 HPCMP funding level throughout the FYDP.

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, NAVY

Items of Special Interest

Navy reimbursable work for other Federal agencies

The committee is aware that the Chief of Naval Operations recently issued guidance to Navy working capital funded entities, including the science and technology laboratories and test and evaluation centers, to cease conducting reimbursable work for other Federal agencies. The committee is concerned that such a moratorium ignores how working capital funded entities operate and the value that outside, reimbursable work can have on reducing the overall rate structure for entities like the naval warfare centers. The committee also believes that such a move could be detrimental to the overall efficiency of the Federal research and test enterprise by forcing other Federal partners to rely on contractors to provide these services, or to build additional, redundant scientific and test capabilities. For example, the Department of Homeland Security works very closely with the naval warfare centers to provide science, technology, test and evaluation capabilities for its programs, and without that support, the Department of Homeland Security would have to devote a larger percentage of its research, development, test, and evaluation budget to providing those services itself.

Therefore, the committee directs the Secretary of the Navy, in coordination with the Chief of Naval Operations, to provide a briefing to the House Committee on Armed Services by March 1, 2015, on the rationale for the decision to cease reimbursable work for Federal agencies outside of the Navy, and an analysis of the policy impacts of this decision, including the ability to facilitate interagency work and fully utilize existing infrastructure. The briefing should also examine the anticipated effect on Navy working capital fund rates if the policy is enforced, as well as the impact if the policy is rescinded. Finally, the briefing should examine the impact on each naval warfare center, and the role of the warfare center's commanding officers in making decisions related to reimbursable work.

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

Items of Special Interest

Analysis of Alternatives for Undersea Clandestine Insertion of Special Operations Forces

The committee is aware of a recently completed Analysis of Alternatives (AOA) for Undersea Clandestine Insertion of Special Operations Forces and that the review provides alternatives for continued operational capability as well as future growth for Navy Sea, Air, Land undersea insertion capabilities. The committee understands that this AOA included representatives from U.S. Special Operations Command, the Department of the Navy (Program Executive Officer, Submarines), and the Joint Staff and was coordinated by a study director from the RAND Corporation, a Federally Funded Research and Development Center. The committee understands that the final publication of the AOA was to be made available to the congressional defense committees in March 2014.

Therefore, the committee directs the Secretary of Defense to provide a copy of the Analysis of Alternatives report in its entirety and a briefing on the report to the congressional defense committees by July 1, 2014. The report and briefing should be presented to the committees in unclassified and classified formats as determined by the Secretary of Defense.

Biosecurity in Department of Defense research facilities

The committee is concerned about the potential threat posed to the United States by biological weapons. The threat of a biological attack may come from a number of sources, including state, non-state and even lone actors, as was believed to be the case in the 2001 Anthrax attacks. The Subcommittee on Intelligence, Emerging Threats and Capabilities held a hearing on October 11, 2013, that examined the state of U.S. efforts for biodefense. During that hearing, the panel of independent expert witnesses was critical of the biosafety and biosecurity procedures in medical research facilities, identifying a lapse of proper screening and consistent procedures as a potential risk with respect to lone actor threats. While the committee notes that the biological agents stored in medical research facilities are not the only source of weaponizable materials, the committee believes the Department of Defense should take all precautions possible to mitigate the risk of bioterrorism.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the Committee on Armed Services of the House of Representatives not later than September 30, 2014, on biosecurity procedures within Department of Defense biological research facilities which handle or store Category A, B, or C priority pathogens. The briefing should include a discussion of personnel screening procedures, security procedures, and the means for training personnel on safety and

security procedures. The briefing should also highlight any inconsistencies or variability in procedures across the facilities.

Chemical Biological Defense Program threat priorities

The committee is aware of significant efforts within the Chemical Biological Defense Program (CBDP) to develop medical countermeasures to protect U.S. troops from chemical, biological, radiological and nuclear (CBRN) threats. The committee notes that the development of a drug or vaccine to treat or protect against a given threat in many cases will take up to a decade from the time of conception through the Food and Drug Administration approval process to be available for use. However, the committee recognizes that the CBRN threat space is constantly evolving in terms of the type and severity of threats U.S. troops are likely to encounter at any point in time. The committee is concerned about the mismatch in these timescales, and therefore directs the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs to brief the House Committee on Armed Services by September 30, 2014, on the approved process for establishing and validating the priorities for the threats for medical countermeasures research and development. The briefing should include a list of the current threats, and the frequency with which the priority list is updated.

Coordination of efforts for advanced manufacturing of medical countermeasures

The committee is aware of multiple efforts in biological defense within several Government departments and agencies, in particular in the area of medical countermeasures (MCM). The Chemical Biological Defense Program (CBDP) within the Department of Defense has begun construction on an advanced manufacturing center for MCM in order to address the unique needs of the Department of Defense for medical countermeasures. However, the committee is also aware that the Department of Health and Human Services has also made significant investments in constructing its own centers for advanced manufacturing. In general, these centers will be focused on addressing the requirements of the Department of Health and Human Services for MCM.

In testimony before the Subcommittee on Intelligence, Emerging Threats and Capabilities on October 11, 2013, the principal investigator for the Texas A&M Center for Innovation in Advanced Development and Manufacturing, one of the Department of Health and Human Services centers, testified that those centers were fully capable of meeting all Department of Defense requirements for MCM advanced manufacturing. This has raised questions regarding the need for the Department of Defense to fund what appears to be a duplicative effort. The committee notes that while there are differences in the capabilities between the Department of Defense and Department of Health and Human Services centers, there is also a significant amount of overlap.

The committee is aware that coordination on research and development of MCM is performed through the Public Health Emergency Medical Countermeasures

Enterprise (PHEMCE), in which the Department of Defense is an active participant. These coordination efforts are laudable. However, the committee is aware that the PHEMCE is not directly managing the advanced manufacturing process and will instead rely on a separate governance board. In light of these facts, the committee is concerned that, although the Department of Defense center for advanced manufacturing is already designed and construction has begun, the ability to coordinate with and leverage the efforts of other Government agencies for advanced manufacturing does not yet appear to be fully established, and therefore, the possibility of inefficiency and unnecessary redundancy within the Department of Defense is still significant.

Therefore, the committee directs the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs to provide a briefing to the congressional defense committees by October 30, 2014, on the status of the coordination process for the advanced manufacturing of medical countermeasures between the Department of Defense and the Department of Health and Human Services. This briefing should include the following:

(1) Details of the Department of Defense's role on the governance board which oversees the advanced manufacturing process, including frequency of meetings, level of interaction, etc.

(2) The degree to which the Department of Defense is able to utilize the Department of Health and Human Services advanced manufacturing centers, including a discussion of time and cost savings.

(3) Any application of best practices, lessons learned, etc. from past coordination efforts with the PHEMCE with respect to the current coordination efforts for advanced manufacturing.

(4) Any obstacles to the coordination process, including any issues which may prohibit or impede the Department of Defense's ability to utilize the Department of Health and Human Services advanced manufacturing centers.

Development of innovative detection and threat identification technologies

The committee remains concerned about credible threats posed by state and non-state actors in their attempts to acquire and weaponize chemical, biological, radiological, nuclear and high-yield explosive (CBRNE) weapons of mass destruction (WMD) for use against the United States and its allies. The committee is aware that the Defense Threat Reduction Agency (DTRA) continues to develop and field technologies that reduce, counter, and eliminate the threat of CBRNE WMD. The committee is also aware that as part of these efforts, DTRA continues to invest in small lightweight, person-portable detection equipment to detect CBRNE materials. The committee recognizes the importance of this equipment as enabling a wide range of operations within CBRNE environments, and therefore encourages DTRA to continue the development, demonstration and deployment of innovative and emerging detection and threat identification technologies that are useful across the widest-spectrum of CBRNE threats. In addition, the committee directs the

Director of DTRA to brief the House Committee on Armed Services by December 31, 2014, on their efforts to advance and make operational a light-weight, person-portable CBRNE detection and analysis device.

Field-programmable gate arrays for defense

The committee recognizes the importance of utilizing field-programmable gated arrays (FPGAs) for defense application in order to allow for greater flexibility in the processing power of some defense applications. The committee is aware, though, that such capability can also introduce vulnerabilities into defense systems, and the Department of Defense is challenged to find means to mitigate those potential vulnerabilities and ensure a high level of trust for this class of microcircuits. Further, the committee notes that the prevalence of foreign FPGA providers makes trusted sourcing for these microcircuits an additional security challenge that the Department must address.

Therefore, the committee directs the Under Secretary of Defense for Acquisition, Technology, and Logistics to conduct an analysis of the Department's strategy for utilizing FPGAs and to provide a briefing to the House Committee on Armed Services by March 1, 2015 on the results of the analysis. The briefing should address the following issues:

(1) How FPGAs fit into both Department's microelectronics strategy, especially with regard to their use in both new and legacy systems;

(2) How trust and security vulnerability can be mitigated by the Trusted Defense Systems strategy;

(3) Any special budgeting, manpower, manufacturing or acquisition issues that may need to be addressed by the use and integration of FPGAs; and

(4) Recommendations for how to increase utilization of FPGAs, and if necessary, production capacity.

Guidance on utilizing non-profit research institutes

The committee recognizes that independent, non-profit research institutions provide value to the research and development portfolios of the Department of Defense. The committee believes that non-profit research institutions have unique capabilities, experience, and infrastructure that are well suited to technology maturation, risk reduction, and transition to programs of record.

As noted in the committee report (H. Rept. 113-102) accompanying the National Defense Authorization Act for Fiscal Year 2014, the committee is aware the Department is examining ways to better utilize the unique capabilities and expertise of non-profit research institutions, especially in the area of transitioning innovation to commercialization. Furthermore, the committee understands that the Department has been evaluating how to better utilize the special authorities within the Defense Federal Acquisition Regulations in order to better leverage the capabilities of the non-profit research community. The committee is concerned that

the Department has not clearly articulated that policy to the broader research and acquisition community to inform them of how they might best leverage those capabilities, and the special contracting authorities that might be used.

Therefore, the committee directs the Secretary of Defense to issue updated policy guidance related to the use of non-profit research institutions that clarifies their role in the research ecosystem, as well as the special provisions within the Defense Federal Acquisition Regulations that support their use. Additionally, the committee directs the Secretary to submit the updated policy guidance to the Committees on Armed Services of the Senate and House of Representatives by March 1, 2015.

Health of the research and development enterprise

The committee remains concerned about the long-term health of the Department of Defense research and development enterprise. There are currently 67 Department laboratories across 22 states, 10 federally funded research and development centers (FFRDCs), and 13 university affiliated research centers, as well as a workforce of 60,000 employees, of which approximately 36,400 are degreed scientists and engineers. The committee recognizes the pivotal role these facilities and people play in maintaining the technological edge of the Department of Defense and providing the necessary tools for the warfighter. The committee is concerned that the declining state of much of the Department of Defense lab infrastructure, especially compared to academic, industrial, and international counterparts, can also serve to dispel many of the technology workforce that the Department would most like to attract.

The committee is determined to ensure that Department research and development capabilities remain robust in order to assure a vibrant and agile research and development enterprise. The committee is concerned that declining budgets and increasing threats are placing pressures on the Department that may lead it to make short-term decisions with long-term ramifications. The committee is unsure if the Department is striking the appropriate balance between near- and long-term objectives, which may negatively affect the overall health of the research and development enterprise.

Therefore, the committee directs the Secretary of Defense to task the Defense Science Board to conduct an assessment of the organization, missions, authorities, and health of the defense research and development enterprise, and to submit a report on the findings of the assessment to the congressional defense committees by September 30, 2015. The assessment should include the following:

(1) How well do the defense laboratories respond to the needs of the Department?

(2) What mechanisms exist to refurbish and recapitalize Department of Defense labs, and how do those mechanisms compare with other Government, academic, international and industrial counterparts?

(3) How well does the Department attract, recruit, retain, and train its workforce to remain technically current and flexible to respond to emerging national requirements?

(4) Does the appropriate balance exist in each service between service control and laboratory director discretion so as to maximize laboratory mission effectiveness?

Internet access on Kwajalein Atoll

The committee is aware that the Department of Defense maintains a significant presence on Kwajalein Atoll, including contractors and families, to support Department of Defense activities there. Further, the committee understands that data access for those families is limited to low-bandwidth phone modems, which can negatively impact the welfare of personnel and their families stationed at a remote location, where electronic communications are useful in maintaining personal and family relationships.

Furthermore, the committee notes that the Defense Information Systems Agency (DISA) maintains high-bandwidth network connections to the Atoll, which were designed with additional capacity to allow for future expansions. The committee is also aware of instances in the past when DISA has provided additional networking capacity for morale, welfare and recreation applications through base exchanges. The committee believes that DISA could provide such capacity to families on the Atoll with minimal effort and cost. Therefore, the committee directs the Director, Defense Information Systems Agency to submit a plan to the Committee on Armed Services of the House of Representatives by March 15, 2015, on providing internet access to families on Kwajalein Atoll.

Military service coordination and transition efforts for the chemical biological defense program

The Chemical Biological Defense Program (CBDP) has the primary responsibility to develop technologies to protect U.S. troops from the threats posed by Chemical Biological Radiological Nuclear and Explosive (CBRNE) Weapons of Mass Destruction (WMD). The committee believes that frequent open communication between the CBDP and the military services is critical during all phases of the research, development, test, and evaluation (RDT&E) process for developing these technologies. Such communication is necessary to ensure not only that the warfighter requirements are being properly addressed in the early planning phases of the RDT&E process, but that the technology is transitioned to the military services on an adequate timescale to ensure the safety and protection of U.S. troops. Therefore, the committee encourages the CBDP to continue to improve its communication with the military services during all phases of the RDT&E process.

In addition, the committee remains concerned about the level of protection currently available to U.S. troops who are at risk of being exposed to CBRNE WMD,

in particular with regards to mission-oriented protective posture (MOPP) gear. The committee is concerned that in many cases the equipment available to the military units may be outdated or inadequate to address current requirements. Therefore, the committee directs the Assistant Secretary of Defense for Nuclear, Chemical and Biological Defense Programs to provide a briefing to the House Committee on Armed Services by November 30, 2014, on the coordination between the military services and the CBDP. The briefing should include details on the process by which the CBDP solicits and incorporates input from the military services into its planning and prioritization of RDT&E efforts, as well as the current plans and efforts to transition the resultant technology, including MOPP gear for CBRNE environments to the military services.

Special Operations developmental efforts for Tactical Assault Light Operator Suit

The budget request included $10.0 million in PE 1160402BB, Special Operations Technology Development, and $7.5 million in PE 1160402BB, Special Operations Special Technology, to support ongoing developmental efforts for the U.S. Special Operations Command (USSOCOM) Tactical Assault Light Operator Suit (TALOS), designed to improve operator survivability in direct action or kinetic environments.

The committee notes that more than $4.5 million of fiscal year 2013 and fiscal year 2014 Major Force Program-11 funding has been put towards TALOS efforts thus far. The committee also notes that despite aggressive marketing efforts by USSOCOM, TALOS is not a program of record, but rather "an overarching vision" that provides "a coordinating focus for many of USSOCOM's science and technology efforts spanning multiple capability areas." The committee understands that present efforts are being used to survey current technologies and to better inform future requirements documents, and that USSOCOM intends to deliver a fully functional prototype assault suit by August 2018.

The committee is concerned that these requirements are not being properly coordinated with related or complementary efforts at the Defense Advanced Research Projects Agency (DARPA) and the U.S. Army Natick Soldier Systems Command. While USSOCOM is the proper authority to define Special Operations Forces peculiar requirements, it may not be the appropriate entity to lead such developmental technology efforts, like TALOS. While the committee understands that Natick Soldier Systems Command is currently developing and partially funding one of the two Generation I prototypes for USSOCOM, the committee is concerned that USSOCOM is also funding outside private sector research, and that overall efforts lack proper coordination and oversight, systems integration and collaboration, and prototype evaluation.

Therefore, the committee directs the Secretary of Defense to brief the congressional defense committees by August 1, 2014, on the TALOS project and similar efforts to include: (1) the overall TALOS requirement for U.S. Special Operations Forces, including requirements validation; (2) a list of funded activities

for fiscal years 2013-14, as well as planned activities for fiscal year 2015 and beyond, including efforts through DARPA, Natick Soldier Systems Command, the other military services, the Rapid Innovation Fund, and industry; (3) coordination efforts undertaken with USSOCOM, DARPA, Natick Soldier Systems Command and other similar ongoing research and development activities; (4) project timelines including the development of prototypes and anticipated funding; (5) any other developmental efforts underway that could satisfy USSOCOM TALOS-like requirements, and (6) any other items the Secretary of Defense deems appropriate.

Technologies to improve spectrum efficiency

The committee is aware that spectrum is a vital national security resource which must be actively managed to ensure effective and efficient use that balances competing demands between the military services, other Federal agencies and the private sector. In the committee report accompanying the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (H. Rept. 110-652), the committee noted its concern over the availability of spectrum for defense applications and the increasing scarcity imposed by additional spectrum auctions and competition with commercial wireless providers. For this reason, the committee is pleased that the Department of Defense has recently issued an Electromagnetic Spectrum Strategy to provide more strategic guidance to shape the future of the Department's spectrum operations. As noted in the new strategy, "[the Department of Defense] must act now to ensure access to the congested and contested electromagnetic environment of the future. Specifically, the Department must adapt how it acquires and uses spectrum resources. Our approach must include acquiring more efficient, flexible, and adaptable systems while developing more agile and opportunistic spectrum operations to ensure that our forces can complete their missions."

The committee is also aware that this strategy is the first step in a longer process to develop a roadmap and action plan to inform future actions and resourcing. In addition, the committee believes that the Department needs to identify opportunities where it should focus research and development efforts to address any technological gaps, or where additional testing for commercial technologies may be needed to integrate into defense systems.

Therefore, the committee directs the Chief Information Officer of the Department of Defense to brief the House Committee on Armed Services by January 15, 2015, on the status of the associated Spectrum Roadmap and Action Plan, as well as a science and technology roadmap for technologies that are needed to improve spectrum efficiency.

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

ITEMS OF SPECIAL INTEREST

Comptroller General Review of Department of Defense Trusted Foundry and Supply Chain Risk Management Programs

The committee recognizes that trusted components, both hardware and software, are vital to ensure the security and integrity of defense systems. To that end, the Department of Defense established a Trusted Foundry program to ensure a dedicated supply of trusted microelectronics for highly sensitive defense applications, as well as a trusted supplier program to provide less advanced microelectronics that still require a high degree of trust. The committee also notes that section 254 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110-417) required the Department to develop a Trusted Defense Systems Strategy to ensure that those capabilities were aligned with the policy framework needed to enforce the use of those capabilities.

After 10 years of this capability and policy framework, the committee believes that it is important to review the Trusted Foundry program, the Trusted Suppliers certification program, and other supply chain risk management to determine their effectiveness and understand if updates or changes are necessary. Therefore, the committee directs the Comptroller General of the United States to review and submit a report to the Committees on Armed Services of the Senate and the House of Representatives not later than February 1, 2015, on the Department's program related to trusted foundry, trusted suppliers, and other supply chain risk management activities to ensure that the program strategy, contracting vehicles, and execution are fully supported by clear policy guidance from the Department, that such guidance is being followed, and to make any recommendations for needed improvement.

Independent Assessment of Department of Defense Cloud Computing Acquisition and Brokerage Policies

The committee is aware that there are significant cloud computing resources in the commercial sector that have resulted in reduced data center infrastructure and support personnel, leading to cost savings and efficiency for users of these services. The committee acknowledged that reality, as evidenced by the language in section 2867 of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112-81) that called for a strategy for transitioning to cloud computing, including the utilization of cloud computing services generally available within the private sector.

The committee believes that the Department of Defense could benefit from that trend, but is concerned that the guidance for leveraging commercial cloud services is being developed too slowly. The committee believes that an outside review of the Department's guidance and planning for cloud computing capabilities, including both in-house and private sector, would be valuable. Therefore, the committee directs the Secretary of Defense to conduct an independent assessment of the Department's policies and guidance for cloud computing capabilities and provide a briefing to the Committees on Armed Services of the Senate and the House of

Representatives by September 30, 2015. This assessment should include the following:

(1) Whether industry and government best practices are embodied in Department of Defense policies and guidance;

(2) Whether cloud brokerage procedures are clearly articulated, commonly understood by service providers, and unbiased with respect to the use of in-house government-provided cloud services;

(3) Whether security protocols for commercial cloud products and services are clearly articulated;

(4) Whether guidance exists for integration of commercial cloud capabilities into the architectural plans for the Joint Information Environment; and

(5) Whether the ongoing commercial cloud pilots are being evaluated for cost, performance, and security against standardized, consistent, and objective measures of effectiveness that are adequately aligned with current guidance.

TITLE X—GENERAL PROVISIONS

ITEMS OF SPECIAL INTEREST

OTHER MATTERS

Assessment of Counterfeit Detection Efforts

The committee recognizes the challenges posed to the Department of Defense in identifying and mitigating the presence of counterfeit parts in its supply chain. Section 818 of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112-81) was an important step in establishing policy, guidance, and compliance reporting to move the Department forward in addressing the detection and mitigation of counterfeit parts, including microelectronics. The committee believes that it is important to take stock of the actions that have been taken to date and to evaluate their effectiveness.

Therefore, the committee directs the Under Secretary of Defense for Acquisition, Technology, and Logistics to provide a briefing to the House Committee on Armed Services by December 1, 2014, assessing the approaches currently taken to mitigate counterfeit parts in the supply system. The briefing should include the following:

(1) A cost benefit assessment of current compliance and technology measures for mitigating counterfeit parts, including microelectronics, in the supply chain, and requirements for deoxyribonucleic acid authentication marking. This assessment should include costs associated with program implementation and the scope of components that are being addressed by these measures;

(2) An assessment of the costs and benefits of expanding these measures to additional classes of technology, which have been deemed at high risk for counterfeiting;

(3) An analysis of the quantity of alerts and problem advisories reporting counterfeit electronic parts in the Government Industry Data Exchange Program since January 2011 that were a result of the use of the measures described in item (1) above; and

(4) A description and analysis of the Department of Defense's efforts to collaborate and coordinate with the defense industrial base on the development of standards associated with the prevention, detection, and responses to the threat of counterfeit electronic parts in the military supply system.

Comptroller General Review of Department of Defense Antiterrorism and Force Protection Efforts

The committee recognizes that there have been an increasing number of insider attacks on U.S. military bases in recent years. In November of 2009, 13 people were killed and 43 others wounded when a soldier opened fire at Fort Hood, Texas. The committee notes that following this shooting at Fort Hood, the Secretary of Defense established the Department of Defense Independent Review Related to Fort Hood. The review board presented its findings and recommendations to the Secretary of Defense in January 2010. In completing its review, the review board limited the depth of its study in certain areas, including force protection roles and responsibilities and threat assessment programs, based on the Secretary of Defense's stated intent to have the military departments conduct in-depth follow-on reviews. However, the committee is concerned that more incidents have occurred since this incident, including a shooting at the Washington Navy Yard in September of 2013, as well as a second shooting at Fort Hood in April of 2014.

The committee recognizes that insider attacks, such as these, pose a different challenge to Department of Defense's traditional antiterrorism and force protection efforts that address external threats. Therefore, the committee directs the Comptroller General of the United States to conduct a comprehensive review of the inside-the-wire, antiterrorism and force protection efforts of the Department of Defense, and submit a report to the House Committee on Armed Services by March 30, 2015. The review should address the following areas:

(1) The extent to which the Department of Defense has implemented the recommendations identified in the Department's Independent Review Related to Fort Hood;

(2) The status of the follow-on studies to be completed by the military departments and to what extent have any recommendations from these studies been implemented;

(3) Additional actions taken by individual installations, and the extent to which these efforts have been shared with other installations; and

(4) The extent to which the Department's current antiterrorism and force protection policies, guidance, and standards address insider threats.

Coordination of Efforts to Track and Counter Weapons of Mass Destruction

The committee remains concerned about the threats posed by weapons of mass destruction (WMD) to the safety and security of the United States. Efforts to track and counter WMDs exist within a significant number of Federal agencies. The committee recognizes that counter-WMD missions outside of U.S. borders reside within the purview of the Department of Defense. However within U.S. borders, these missions fall within the jurisdiction of the Department of Homeland Security and the Federal Bureau of Investigation.

The committee notes that as outlined in the 2014 Quadrennial Defense Review, the combating WMD strategy of the Department of Defense is to eliminate WMD threats prior to entering the United States; however, the committee recognizes that this may not always be possible. The committee is concerned about the eventuality wherein a WMD device crosses these jurisdictional boundaries, in particular, in regards to the coordination efforts between the Department of Defense and local, state, and Federal authorities. The committee believes that in the case of such an occurrence, the cooperation between the Department of Defense and other Government agencies should be absolute in order to guarantee the elimination of WMD threats. Therefore, the committee directs the Secretary of Defense to brief the House Committee on Armed Services by September 1, 2014, on the coordination efforts between the Department of Defense, the intelligence community, and local, state, and Federal authorities for tracking and combating weapons of mass destruction entering the United States. The briefing should include details on the authority structures in place within the Department of Defense to facilitate the coordination efforts, as well as examples of how these structures would operate in a realistic threat scenario.

Economic Warfare Policy

The committee continues to be concerned by the possibility of adversaries utilizing economic warfare as a means to undermine U.S. military advantages. As noted in the committee report (H. Rept 112-78) accompanying the National Defense Authorization Act for Fiscal Year 2012, "[t]he committee is concerned that our adversaries understand this dependency, and are developing means to attack our military strength by attacking our economy."

In making those observations, the committee noted the findings of a 2009 report from the Irregular Warfare Support Program titled “Economic Warfare: Risks and Responses,” which offered some plausible scenarios about how economic warfare might be used against the United States. That report also made a number of recommendations which have yet to be given serious attention by the Department of Defense or the national security establishment, including:

(1) Recognize that protecting the American economy and industrial capability is a top defense priority that should be properly funded and supported;

(2) Thoroughly research the hypothesis of economic warfare described from an economic defense perspective; and

(3) Create a specialized threat finance unit to develop and implement appropriate countermeasures to emerging economic warfare threats.

Since that report was released, the committee has become increasingly aware of the potentialities that cyber-enabled technologies add to these economic and financial threats. For example, the large-scale theft of intellectual property in sectors of strategic importance to the United States poses a direct challenge to U.S. technological superiority, but also a long-term economic pressure as we are forced to develop countermeasures against our own stolen defense technologies and potentially lose market advantage in some non-military technology sectors. The presence of large swaths of the financial sector without an adequate monitoring framework that could be exploited by terrorist or nation-state, such as dark trading pools, credit default swaps, sovereign wealth funds, naked short selling, or algorithmic trading, may be a significant blind spot for the United States.

Given the pervasive nature of these threats, and the apparent lack of clear policy guidance or organization to address these issues, the committee directs the Secretary of Defense to provide a report to the Committee on Armed Services of the House of Representatives by August 1, 2015, on the Department's assessment of these activities. The report should include:

(1) Articulation of what sorts of activities amount to economic warfare upon the United States;

(2) Clarification of the roles and responsibilities of the Department of Defense in providing indications and warning of, or protection against, acts of economic warfare;

(3) The current status of authorities and command structure related to economic warfare; and

(4) Recommendations for improving the Department's capabilities, authorities, or command structure, as well as improving its coordination and support for interagency partners in dealing with economic warfare threats.

Information Management Systems for Response Forces

The committee is aware that the National Guard Bureau Weapons of Mass Destruction-Civil Support Teams (WMD-CST) currently field a system called the CST Information Management System, 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 in the National Guard Chemical, Biological, Radiological and Nuclear (CBRN) Response Enterprise, there are also other capabilities such as the Unified Command Suite and the Joint Incident Command Suite. Because each of these tools support different echelons of command with different but related capabilities, it is vital that there be a comprehensive strategy for how to rationalize the current suite of tools, and move forward with a common, interoperable, enterprise information management solution.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by January 15, 2015, on a comprehensive strategy for developing and fielding an information management architecture for the Department's CBRN Response Enterprise. This strategy should define the information architecture needs for the CBRN Response Enterprise as well as its plans to achieve enterprise-wide data interoperability for all operating elements within the Response Enterprise.

Inventory of Counter Threat Finance Programs and Capabilities

The committee recognizes that illicit financial networks are critical enablers to destabilizing networks and transnational criminal organizations, including terrorist, narco-traffickers, human smugglers, proliferators and actors seeking to avoid sanctions. The Department of Defense invested heavily in the Republic of Iraq and the Islamic Republic of Afghanistan to create counter threat finance capabilities to detect and combat such illicit activity. With the draw-down in Afghanistan and the pivot to Asia, the committee is concerned that the Department might begin to divest itself of such counter threat finance capabilities in favor of traditional military capabilities. However, the committee believes such capabilities will continue to be of value to combat threats to our national security, including state actors avoiding sanctions or maintain black market economic activities. The committee also believes such capabilities can be useful in supporting surveillance and indications and warning for national economic threats, such as attempts to perpetrate economic warfare or sabotage. Therefore, the committee directs the Secretary of Defense to provide a report to the Committees on Armed Services of the Senate and the House of Representatives by February 15, 2015, on an inventory and sustainment plan for Department of Defense counter-threat finance programs and capabilities.

Military Auxiliary Radio System

The committee continues to support the Military Auxiliary Radio System (MARS), a Department of Defense-sponsored auxiliary organization of volunteer amateur radio operators who provide contingency communications support to the Department of Defense and U.S. Government operations. In addition to providing an important back-up to conventional communications that is potentially vulnerable to disruption or degradation, MARS can play a vital role in helping to ensure continuity of Government and continuity of operations in the event of a natural or man-made disaster. Given these advantages of MARS, the committee is concerned by the Department's lack of action in fully utilizing this capability. In the committee report (H. Rept. 112-479) accompanying the National Defense Authorization Act for Fiscal Year 2013, the committee encouraged the Department to clarify and maintain policy oversight of MARS within the Office of the Secretary of Defense and to update Department of Defense Instruction (DODI) 4650.02 entitled "Mars Auxiliary Radio System (MARS)" with respect to the

disestablishment of the Office of the Assistant Secretary of Defense for Networks and Information Integration. The committee notes, however, that these actions have not yet occurred.

The committee is aware of efforts to revise and update DODI 4650.02, which establishes policy, procedures, and responsibilities for MARS. However, the revision is not yet complete. Therefore, the committee directs the Secretary of Defense to ensure that any rewrite of the DODI 4650.02 effectively integrates MARS into the Department of Defense's emergency communications plan; consolidates MARS operations through appointment of an individual MARS manager to ensure standardization of operating policies and procedures among the three MARS branches within the Army, Air Force, and Navy-Marine Corps; and directs the service secretaries and geographic combatant commanders to integrate MARS more fully into their operational planning and activities. In addition, the committee directs the Secretary of Defense to brief the Committee on Armed Services of the House of Representatives by August 30, 2014, on the status of the revision of DODI 4650.02.

Review of Military Standard to Protect Systems Against Electromagnetic Pulse

The committee is aware that the Department of Defense maintains a military standard for protection of ground-based systems and facilities performing critical and time-urgent command, control, communications, computer, and intelligence missions from high-altitude electromagnetic pulse (HEMP). This military standard, known as MIL-STD 800-125-1 and -2, details the performance, acceptance test, and verification test requirements for identified systems, as well as HEMP-unique acceptance and verification test techniques.

The committee is concerned that in the nearly 16 years since this standard was last updated, technology may have progressed in ways that have out-paced the ability of the standard to ensure protection of designated systems. For example, on the offensive side, the capability exists now to buy commercial-off-the-shelf, non-nuclear electromagnetic pulse (EMP) generators to provide EMP effects without the need for nuclear devices. On the defensive side, the higher reliance on commercial information technology hardware, and the interconnection of such systems, results in a more complex interaction between specific systems that must be characterized to understand the propagation of EMP effects.

Therefore, the committee directs the Secretary of Defense to conduct a review of MIL-STD 800-125-1 and -2 to determine if the standards are in need of updating based on the current and future projected threats, and whether the Department needs to revise the frequency for revisiting testing against these standards to ensure changes or updates to systems and facilities have not opened up new vulnerabilities. Additionally, the committee directs the Secretary to provide a briefing to the Committee on Armed Services of the House of Representatives by June 1, 2015, on the results of this review.

Spectrum Operations Centers

The committee is aware that U.S. Strategic Command operates the Joint Electronic Warfare Center (JEWC) at Lackland Air Force Base, Texas. An important aspect of the JEWC is its role in connecting electronic warfare (EW) resources to the warfighter, and the committee believes that the JEWC provides critical operational EW support to the combatant commands, including combat operations support, opposing force EW during operational training exercises, Joint and North Atlantic Treaty Organization EW reprogramming, joint capabilities technology demonstration support and modeling analysis and simulation.

The committee believes that the capabilities of the JEWC could be enhanced by having connections with sister organizations within each of the military services to act as spectrum coordination centers that would coordinate service-specific resources and needs into the planning and operations of the individual service training, exercises, and operations. Therefore, the committee directs the Secretary of Defense, in coordination with the Secretaries of the military departments, to provide a briefing to the House Committee on Armed Services by June 1, 2015, that describes the use case for such spectrum operations centers, as well as a business-case analysis for designating or developing organizations to act in such a role. The briefing should examine the relative costs and benefits of leveraging existing organizations, as well as how such an organization could support full-scope electromagnetic operations, including EW, spectrum management, and cyberspace operations.

Standing Joint Force Headquarters for Elimination

The committee is aware that as a result of direction received in the 2010 Quadrennial Defense Review, U.S. Strategic Command (STRATCOM) established the Standing Joint Force Headquarters for Elimination (SJFHQ-E) in 2012 with the purpose of planning, training for, and executing command and control functions during weapons of mass destruction (WMD) elimination missions. However, the committee believes that the planning and training mission of the SJFHQ-E appears to have significant overlap with the STRATCOM Center for Combating WMD (SCC-WMD), which performs a similar function for the larger mission space of combating WMD. The committee is also aware that prior to the formation of the SJFHQ-E, the command and control functions for elimination missions were performed through the establishment of a Joint Task Force for Elimination (JTF-E), which was only established if and when it was deemed necessary based on the scope of the elimination mission. In addition, the committee notes that in its formation, the SJFHQ-E assumed the tasks, missions, and operations of the Joint Elimination Coordination Element (JECE) which previously functioned as the core of any JTF-E upon its formation.

The committee believes that combating and eliminating WMD is of the utmost importance for national security. However, the committee also believes that in the current austere fiscal climate, the additional cost and bureaucracy associated with a standing headquarters must provide necessary, differentiable capability.

Therefore, the committee directs the Secretary of Defense to brief the House Committee on Armed Services by September 30, 2014, on the added benefit of the SJFHQ-E. The briefing should discuss unique value added by the formation of a standing headquarters, and compare the current capabilities and associated costs of the SJFHQ-E with those capabilities that existed previously among the SCC-WMD and the existing JECE.

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

ITEMS OF SPECIAL INTEREST

Non-Lethal Weapons for Contingency Operations

The committee reaffirms its longstanding support for the accelerated development, fielding, and deployment of non-lethal technologies. Non-lethal systems are useful for both force application and force protection missions. The committee notes that their employment is consistent with U.S. military strategy and helps minimize damage to property and inadvertent civilian casualties in the kinds of operational contingencies, including irregular warfare and humanitarian crises, in which U.S. forces are likely to be engaged. Their use provides commanders with additional decision time and space before resorting to lethal force, helps mitigate the negative consequences of unintended non-combatant injuries and fatalities, and enhances the overall prospects of mission success.

The committee understands that, as a result of budget pressures, the Department of Defense is proposing significant cuts to the Department's Non-Lethal Weapons program over the next 5 years. This includes a roughly one-third reduction in fiscal year 2015 for overall Department of Defense non-lethal investments and more than a 40 percent reduction in the Future Years Defense Plan compared to the previous 5-year estimate. The committee is also concerned that significant cuts to service procurements are also planned, further exacerbating cuts to the joint program.

The committee believes that such reductions may have unintended or unforeseen impacts on contingency planning related to humanitarian relief, non-combatant evacuation operations, and peacekeeping. If current contingency plans are predicated on the availability of such non-lethal systems, the Department of Defense may be forced into relying solely on lethal force to deal with these emerging requirements. Accordingly, the committee directs the Chairman of the Joint Chiefs of Staff to provide a briefing to the House Committee on Armed Services by February 1, 2015, on the impact of funding reductions for non-lethal systems on current contingency operations planning supporting humanitarian relief, non-combatant evacuation operations, and peacekeeping. This briefing should examine current contingency planning to determine if the level of investment estimated across the Future Years Defense Program in the joint and service programs is

sufficient to support those plans, and a possible course of action to mitigate any shortfall.

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

ITEMS OF SPECIAL INTEREST

Air Force Cyber

The committee notes that the fiscal year 2015 budget request is generally characterized by reductions in most mission areas except cyber. This trend is true across all the military services, including the Air Force. However, the committee believes that for the Air Force, it is particularly difficult to understand the breadth and depth of investment and focus in cyber given the dispersion of cyber manpower across multiple program areas and operating environments.

The committee is concerned that disaggregating the cyber workforce across multiple expenditure centers and projects in such a manner not only makes understanding the entirety of the cyber investment more difficult, it generates greater risk for suboptimizing the cyber workforce, increased unintentional redundancy in tasking, and challenges in managing operational roles and responsibilities.

Therefore, the committee directs the Secretary of the Air Force, in coordination with the Director of the National Security Agency, to provide a report to the congressional defense committees, the Permanent Select Committee on Intelligence of the House of Representatives, and the Select Committee on Intelligence of the Senate by February 16, 2015, that captures the aggregate Air Force investment in cyber, laying out where the various elements of Air Force cyber are nested, and how those elements are integrated within the overall Air Force and Department of Defense cyber enterprises. The report should focus both on the current laydown of personnel as well as the envisioned end-state manning construct. It should also include a discussion on how the Air Force has constructed the various operational chains of command within the service and between the service elements and United States Cyber Command.

Air Force Distributed Common Ground/Surface System

The Air Force Distributed Common Ground/Surface System (DCGS-AF) is a family of existing and planned systems providing multi-intelligence tasking, processing, exploitation, and dissemination capabilities at the Joint Task Force level and below. The committee notes that the fiscal year 2015 request for DCGS-AF totaled $782.4 million dollars and included over 7,600 personnel. Resident in the Processing and Exploitation expenditure center, DCGS-AF has traditionally been viewed in that functional context.

The committee is concerned that through the course of supporting combat operations over the past 12 years, DCGS-AF has begun to evolve beyond the intelligence processing and exploitation functions to include single-intelligence and even multi-intelligence source analysis. The committee believes this presents an important opportunity for the Air Force to clarify the operational role of the DCGS-AF enterprise, taking every measure to ensure full coordination between enterprise elements and complete deconfliction of functions, tasking, and mission responsibilities where possible.

The committee is specifically concerned that initiatives like the DCGS-AF Analysis and Reporting Team (DART) System risk stepping beyond the appropriate functional boundaries for the system, unduly broadening the mission, and distracting the operational focus. However, the committee believes that the future Analysis and Targeting Wing must take full advantage of technical advances accomplished within the DCGS-AF as part of Air Force efforts to clarify and cement appropriate mission assignments across the intelligence enterprise.

Therefore, the committee directs the Secretary of the Air Force to provide a report to the congressional defense and intelligence committees by June 1, 2015, that describes the future of DCGS analytic and processing, exploitation, and dissemination responsibilities. The report should describe which intelligence functions, such as processing, exploitation, and analysis, should reside at the service intelligence centers, the Joint Intelligence and Operations Centers, and at DCGS-AF nodes. The report should outline a proposed Plan of Action and Milestone to execute the transformation to the stated end state, including anticipated costs and manpower requirements across the enterprise and a plan for satisfying those requirements.

Comptroller General Assessment of U.S. Cyber Command

The committee notes that according to the Secretary of Defense, cyberspace is the new terrain for warfare where adversaries seek to do harm to the Nation, the economy, and its citizens. Adversaries, such as nations, insiders, terrorists, criminal groups, hackers, and other individuals and organizations, use an array of cyber tactics that could threaten our nation's security. The unique nature of cyber-based attacks can vastly enhance their reach and impact. To address these threats, the Department of Defense established U.S. Cyber Command as a sub-unified command under U.S. Strategic Command.

In 2010 and 2011, the Government Accountability Office (GAO) reported that the Department's and U.S. Cyber Command's efforts could benefit from additional detail and clarity and that they had not fully defined long-term mission requirements and desired capabilities to guide the military services' efforts to recruit, train, and provide forces with appropriate skill sets. In 2014, GAO also reported on the Department's planning efforts to maintain continuity of operations in a degraded cyber environment.

U.S. Cyber Command achieved full operational capability in October 2010, and is currently responsible for planning, coordinating, integrating, synchronizing, and conducting activities to direct the operations and defense of specified Department of Defense information networks, and to prepare to conduct full spectrum military cyberspace operations, when directed, to enable actions in all domains and ensure U.S. and allied freedom of action in cyberspace while denying the same to our adversaries. As U.S. Cyber Command continues to develop and grow, it is essential that it does so as efficiently and effectively as possible. Accordingly, the committee directs the Comptroller General of the United States to submit a report to the congressional defense committees by March 31, 2015, on the organization, missions, and authorities of U.S. Cyber Command and its operational relationship with the geographic combatant commands. This report should include a review of the existing organizational structure of the U.S. Cyber Command, including the extent to which:

(1) The Department has clearly defined U.S. Cyber Command's mission, responsibilities, and authorities;

(2) U.S. Cyber Command's organization, personnel, and structure support cyberspace operations and leverage relationships with the combatant commands, military services, and defense while minimizing potential overlap or duplication of effort;

(3) U.S. Cyber Command coordinates and supports the operations and activities of the geographic combatant commands, including identifying the offensive and defensive cyber rules of engagement for U.S. Cyber Command and geographic combatant commands and conducting assessments to identify needed cyber capabilities; and

(4) Effective coordination mechanisms have been established between U.S. Cyber Command and other Federal agencies that have a role in cyberspace operations.

Comptroller General Assessment on Airborne Intelligence, Surveillance, and Reconnaissance

Airborne intelligence, surveillance, and reconnaissance (ISR) systems provide critical insight to the warfighter across the spectrum of operations from combat to peacetime. Commanders of the combatant commands recognize the advantages that ISR provides, and therefore have significant demand and requirements for the use of these platforms in their areas of operation. The military departments must balance the warfighter requirements and overall investments to meet a broader defense strategy. Addressing the appropriate level of ISR capacity and capability appears to be a significant and recurring challenge for the Department of Defense.

Therefore, the committee directs the Comptroller General of the United States to assess the processes by which the Department determines its airborne intelligence, surveillance, and reconnaissance investments and balances capability

and capacity in order to meet commanders of the combatant commands' critical ISR requirements. The Comptroller General should provide a report to the congressional defense and intelligence committees by February 1, 2015. The report should address the extent to which the Department of Defense has the necessary:

(1) Risk and resource management structures in place to validate, prioritize, and address airborne ISR collection requirements of the commanders of the combatant commands;

(2) Airborne ISR capabilities to meet current intelligence requirements of the commanders of the combatant commands;

(3) Airborne ISR investment strategy, including the appropriate capability and capacity of platforms and sensors relative to current and anticipated intelligence requirements of the commanders of the combatant commands; and

(4) Any related matters the Comptroller General finds appropriate.

Comptroller General Evaluation on Department of Defense Efforts to Protect Information and Systems from Insider Threats

The committee is aware that the Department of Defense has implemented a number of measures, both technical and administrative, to try to mitigate the threat from privileged insiders. That process began with the unauthorized disclosures from Bradley Manning, but clearly gaps continue to exist that have been exploited by Edward Snowden. The committee remains concerned that the Department's efforts have not been comprehensive enough or implemented swiftly enough to get ahead of the problem. The committee is also concerned that the Department does not have an adequate baseline or rigorous metrics to assess the effectiveness or performance of the measures that are in place.

Therefore, the committee directs the Comptroller General of the United States to submit a report to the congressional defense committees by January 15, 2015, evaluating the Department's efforts at protecting against insider threats. This report should address the following issues:

(1) To what extent has the Department assessed and mitigated for the threat, vulnerabilities, and consequences that insiders pose to Department of Defense information and systems the Department uses?

(2) To what extent has the Department developed and implemented an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force?

(3) To what extent have lessons learned from prior insider threat incidents been incorporated into the Department’s insider threat detection and prevention program?

(4) Has the Department reached out to other Federal agencies, foreign governments, or the private sector to identify best practices and lessons learned with regard to insider threats; and to what extent have those best practices and lessons learned been incorporated into the Department’s insider threat detection and prevention program?

(5) How well has the Department been performing on the assessments, both self-assessments and external assessments, called for in Executive Order 13587; and to what extent has the Department developed corrective action plans to address the findings in a timely manner?

(6) What additional areas need to be addressed, either by technical systems or additional policies?

Defense Intelligence Priorities

As part of both the Department of Defense and the Intelligence Community (IC), the Defense Intelligence Agency (DIA) is dually tasked with providing intelligence collection, analysis, and support specifically responsive to the Department of Defense as well as national requirements established through the National Intelligence Priorities Framework (NIPF). The committee believes that both roles are critical, but can be difficult to balance. The committee also understands that measuring satisfaction of NIPF requirements may be easier than measuring the satisfaction of Department-specific requirements. In part, the committee believes this is due to difficulties with identifying Department-specific requirements in a holistic manner.

Section 922 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113-66) requires the Secretary of Defense to establish a written policy governing the internal coordination and prioritization of intelligence priorities of the Office of the Secretary of Defense, the Joint Staff, the combatant commands, and the military departments to improve identification of the intelligence needs of the Department of Defense. Given this new policy, the committee directs the Director, DIA, to provide an assessment to the congressional defense and intelligence committees by October 1, 2014, of the following:

(1) A specific description of how the new policy is being implemented in terms of driving and focusing DIA intelligence efforts to support the Department;

(2) How efforts to incorporate the new policy are being balanced with DIA's responsibilities pursuant to the NIPF;

(3) The extent to which any other Department of Defense or IC policies or guidance impact DIA's implementation of the new policy; and

(4) Any recommendations to further improve the Department's identification of its specific requirements and DIA's ability to respond to such requirements.

Geospatial Intelligence for Disadvantaged Users

The committee is aware of the stated National Geospatial-Intelligence Agency (NGA) strategic goal to provide online, on-demand access to geospatial-intelligence knowledge. However, in contrast to online products, the committee notes the importance of NGA's continued support to combat forces operating in disconnected, intermittent, and limited bandwidth operational environments.

While current programs are addressing this requirement, a strategic plan for this area has yet to be developed.

Therefore, the committee directs the Director of the National Geospatial-Intelligence Agency, in coordination with the Department of Defense Chief Information Officer, to jointly provide a briefing to House Committee on Armed Services by December 1, 2014, on a joint plan to address the relevant combat forces requirements to efficiently and cost-effectively access national geospatial-intelligence data in disconnected, intermittent, and/or limited bandwidth environments.

Inspector General Review of the Activities Supporting the Joint Information Environment

The committee has been monitoring progress on the Department of Defense's Joint Information Environment (JIE) for several years. The committee is aware that the Department does not consider JIE to be a program of record, but is a coordinating framework for other programs of record in the Department. The committee is concerned that without a strong architectural foundation, many acquisition decisions are being made by the military services and Department of Defense agencies without sufficient planning and rigor to ensure that there is transparency and competition in the process. The committee is aware of at least one instance in which the Air Force, despite a court ruling, failed to adhere to necessary contracting and Federal Acquisition Regulation requirements. The committee believes that the current process for contracting components of the JIE lends itself to an over-reliance on sole-source or brand-names contracts, or other decisions made for expediency over competition.

Therefore, the committee directs the Inspector General of the Department of Defense to review Department of Defense noncompetitive information technology contracts to determine whether they were properly justified as sole source, and to provide a briefing on the results of the review to the Committee on Armed Services of the House of Representatives by March 1, 2015. The review should look at a sample of noncompetitive information technology contracts in fiscal years 2013-14, and review of these contracts should determine whether the Department is overly reliant on sole-source, brand-name or other contract types that bypass competition requirements.

Investments for Joint Information Environment Activities

As noted elsewhere in this report, the committee has been monitoring progress on the Department of Defense's Joint Information Environment (JIE) for several years. The committee is aware JIE is an ambitious initiative to consolidate its information infrastructure, but is considered a coordinating framework for other programs of record in the Department and not a program of record itself. However, the committee recognizes that many existing acquisition programs influence, or are

influenced by, the architectural framework being developed by the Department of Defense, in close coordination with each of the military services and defense agencies.

The committee is concerned, however, that the Department cannot readily indicate which programs are affected by the standards and processes being developed for JIE. The committee believes that JIE cannot be effective if the Department does not understand the span of all programs falling under the rubric of JIE, which will effect resourcing, development, manpower, testing, and evaluation. Therefore, the committee directs the Chief Information Officer of the Department of Defense to provide a briefing to the House Committee on Armed Services by March 1, 2015, that identifies all of the major funded activities within each of the military services and defense agencies that currently contribute to JIE, as well as the funding across the Future Years Defense Program, and an integrated master schedule with major milestones for all of the indicated programs.

Military Intelligence Program and Defense Input to the National Intelligence Program

In addition to describing responsibilities with regard to the Military Intelligence Program, section 3038 of title 50, United States Code, describes the Secretary of Defense's responsibilities regarding the National Intelligence Program. Section 3038 requires the Secretary of Defense to "ensure that the budgets of the elements of the intelligence community within the Department of Defense are adequate to satisfy the overall intelligence needs of the Department of Defense, including the needs of the chairman of the Joint Chiefs of Staff and the commanders of the unified and specified commands and, wherever such elements are performing government-wide functions, the needs of other departments and agencies." Further, section 3038 requires the Secretary of Defense to "ensure that the elements of the intelligence community within the Department of Defense are responsive and timely with respect to satisfying the needs of operational military forces." The Secretary also has specific statutory authorities relating to individual elements of the intelligence community that are part of the Department of Defense.

Within the Office of the Secretary of Defense, the Under Secretary of Defense for Intelligence (USDI) is largely responsible for fulfilling these statutory responsibilities on behalf of the Secretary and plays a critical role in ensuring that the intelligence needs of the warfighter are addressed. Specifically, the USDI has taken the lead role in establishing the new policy required by section 922 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113-66) to govern the internal coordination and prioritization of intelligence priorities of the Office of the Secretary of Defense, the Joint Staff, the combatant commands, and the military departments to improve identification of the intelligence needs of the Department of Defense.

Thus, the committee directs the USDI to provide a report to the congressional defense committees and the congressional intelligence committees by

October 1, 2014, that contains a detailed description of how the new policy regarding Department of Defense intelligence priorities has been integrated into resourcing deliberations and planning for the Military Intelligence Program, and how the new policy has been integrated into USDI's representation of the Department of Defense in resourcing deliberations and planning for the National Intelligence Program.

Processing, Exploitation and Dissemination

The committee recognizes that advances in the understanding and application of Object Based Production and Activity Based Intelligence (ABI) have exposed the imperative need for making every ounce of collected and processed intelligence readily accessible to the all-source analyst community in formats that are consistent, shareable, and searchable. The committee is concerned that the military services have been largely absent or excluded from those discussions and working groups. As the services have a significant personnel investment in intelligence, surveillance, and reconnaissance processing, exploitation, and dissemination (PED), it is of critical importance that they remain abreast of technical advances in shared intelligence and analytic processes. To obtain the maximum possible value from nascent ABI analytic methodologies, the committee believes that every PED process must deliver accurately tagged and accessible or shareable content.

Therefore, the committee directs the Under Secretary of Defense for Intelligence to submit a report to the congressional defense and the congressional intelligence committees by May 1, 2015, on a proposed way ahead for transforming the existing Department of Defense PED enterprise. The report should look across all PED organizations in the enterprise and focus on today's single source products developed in largely single intelligence discipline environments. The report should include a plan of action and milestones (POA&M) laying out specific actions to be taken, by each intelligence disciple and each collector, to evolve or enhance today's PED processes and outputs to a condition that directly facilitates ABI analysis. In building the POA&M, the report should prioritize collection sources, identifying those that can be tackled simultaneously, and highlighting any obstacles that prevent the required PED maturation.

Space-Based Reconnaissance

The committee believes that the Operationally Responsive Space-1 (ORS-1) satellite has provided significant intelligence value to the U.S. Central Command and the Army's 513th Military Intelligence Brigade. When referring to this capability, the 513th stated "the ability to provide timely geospatial-intelligence (GEOINT) response to a real world mission during execution cannot be matched." U.S. Central Command provided similar feedback on the operational flexibility provided by this space reconnaissance asset to support urgent, short-notice requirements.

The committee is aware that ORS-1 is currently operating well beyond its design life, and there is no follow-on program planned. The committee would like to understand the requirements of the commanders of the combatant commands for use of space reconnaissance assets. Therefore, the committee directs the Chairman of the Joint Chiefs of Staff to provide a report to the congressional defense and the congressional intelligence committees by January 15, 2015, on the feedback from each of the commanders of the combatant commands on the utility of space-based reconnaissance capabilities to meet their priority intelligence requirements and their current ability to utilize and control space-based reconnaissance to meet those requirements.

Targeting Enterprise

The committee recognizes the importance of geospatial intelligence (GEOINT) support to military operations. The National Geospatial-Intelligence Agency (NGA) defines GEOINT as the exploitation and analysis of imagery and geospatial information that describes, assesses and visually depicts physical features and geographically referenced activities on the Earth. An important aspect of GEOINT operations is the target material provided to support the common operational picture, mission planning, precision coordinate generation, and other analytical products. The committee believes that the targeting mission is of critical importance, and the current threat environment will create challenges and necessitate the need for further review of the methods to accomplish this mission.

Therefore, the committee directs that the Under Secretary of Defense for Intelligence, in coordination with the Director, National Geospatial-Intelligence Agency, to provide a briefing to the Committee on Armed Services of the House of Representatives and the Permanent Select Committee on Intelligence of the House of Representatives by May 1, 2015, on the state of the targeting enterprise. The briefing should include: an assessment of the current GEOINT targeting capabilities; identification of targeteer training as well as the current and projected number of targeteers across the Defense Intelligence Enterprise, including NGA; and an analysis of opportunities for improvement within the defense intelligence community.

U.S. Transportation Command Joint Intelligence and Operations Center

The U.S. Transportation Command Joint Intelligence and Operations Center (JIOC-TRANS) recently executed a highly successful proof of concept associated with a new organizational construct titled the Transportation Intelligence Center (TIC). While the committee supports the Chairman of the Joint Chiefs of Staff delegation of authority to the TIC to allow full exercise of appropriate intelligence coordination activities as demonstrated in the proof of concept, the committee requires additional information regarding why it is necessary to engender a new organizational construct to achieve the desired end state, particularly when manned with the same personnel as the existing JIOC.

Therefore, the committee directs that the Chairman of the Joint Chiefs of Staff, in coordination with the Director, Defense Intelligence Agency, to provide a report to the congressional defense and the congressional intelligence committees by February 16, 2015, detailing the authorities delegated to the TIC as part of the proof of concept and presenting an evaluation of any obstacles to delegating those same authorities directly to the Commander, JIOC-TRANS. The report should identify any opportunities to apply the same lessons and delegations across the other functional JIOCS (e.g. U.S. Strategic Command JIOC, U.S. Cyber Command JIOC, and U.S. Special Operations Command JIOC) to achieve improved operational intelligence efficiency and effectiveness. Finally, the report should explore the potential for such initiatives to allow more efficient utilization of JIOC or Intelligence Community manning.