H.R. 1960—FY14 NATIONAL DEFENSE AUTHORIZATION BILL

SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS AND CAPABILITIES

SUMMARY OF BILL LANGUAGE 1

BILL LANGUAGE 13

DIRECTIVE REPORT LANGUAGE 61

SUMMARY OF BILL LANGUAGE

Table Of Contents

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS
TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION
LEGISLATIVE PROVISIONS
SUBTITLE B—PROGRAM REQUIREMENTS, RESTRICTIONS, AND LIMITATIONS
Section 2xx—Limitation on Availability of Funds for Air Force Logistics Transformation
Section 2xx—Limitation on Availability of Funds for Defensive Cyberspace Operations of the Air Force
Section 2xx—Limitation on the Availability of Funds for the Program Manager for Biometrics of the Department of Defense
SUBTITLE E—OTHER MATTERS
Section 2xx—Extension of Authority to Award Prizes for Advanced Technology Achievements
Section 2xx—Five-Year Extension of Pilot Program to Include Technology Protection Features During Research and Development of Certain Defense Systems
Section 2xx—Establishment of Cryptographic Modernization Review and Advisory Board
TITLE III—OPERATION AND MAINTENANCE
LEGISLATIVE PROVISIONS
SUBTITLE F—LIMITATIONS AND EXTENSIONS OF AUTHORITY
Section 3xx—Revision to Requirement for Annual Submission of Information Regarding Information Technology Capital Assets
TITLE VIII—ACQUISITION POLICY, ACQUISITION MANAGEMENT, AND RELATED MATTERS
LEGISLATIVE PROVISIONS
SUBTITLE A—ACQUISITION POLICY AND MANAGEMENT
Section 8xx—Modification of Reporting Requirement for Department of Defense Business System Acquisition Programs when Initial Operating Capability is not Achieved within Five-Years of Milestone A Approval
TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT
LEGISLATIVE PROVISIONS
SUBTITLE A—DEPARTMENT OF DEFENSE MANAGEMENT
Section 9xx—Revised Definition for Legacy Systems in Defense Business Enterprise Architecture
SUBTITLE C—INTELLIGENCE-RELATED ACTIVITIES
Section 9xx—Department of Defense Intelligence Priorities
Section 9xx—Defense Clandestine Service

Section 9xx—Revision of Secretary of Defense Authority to Engage in Commercial Activities as Security for Intelligence Collection Activities
SUBTITLE E—CYBERSPACE-RELATED MATTERS
Section 9xx—Mission Analysis for Cyber Operations of Department of Defense
TITLE X—GENERAL PROVISIONS
LEGISLATIVE PROVISIONS
SUBTITLE D—COUNTERTERRORISM
Section 10xx—Modification of Regional Defense Combating Terrorism Fellowship Program Reporting Requirement
SUBTITLE F—STUDIES AND REPORTS
Section 10xx—Strategy for Future Military Information Operations Capabilities
SUBTITLE H—OTHER MATTERS
Section 10xx—Reduction in Costs to Report Critical Changes to Major Automated Information System Programs
Section 10xx—Enhancement of Capacity of the United States Government to Analyze Captured Records
Section 10xx—Review and Assessment of United States Special Operations Forces and United States Special Operations Command
Section 10xx—Inclusion in Annual Report of Description of Interagency Coordination relating to Humanitarian Demining Technology
Section 10xx—Protection of Tier One Task Critical Assets from Electromagnetic Pulse and High-Powered Microwave Systems
TITLE XI—CIVILIAN PERSONNEL MATTERS
LEGISLATIVE PROVISIONS
SUBTITLE A—GENERAL PROVISIONS
Section 11xx—Extension of Program for Exchange of Information-Technology Personnel
Section 11xx—Revision to Amount of Financial Assistance under Department of Defense Science, Mathematics, and Research for Transformation (SMART) Defense Education Program
TITLE XII—MATTERS RELATING TO FOREIGN NATIONS
LEGISLATIVE PROVISIONS
SUBTITLE __—MATTERS RELATING TO AFGHANISTAN POST 2014
Section 12xx—Defense Intelligence Plan
SUBTITLE D—REPORTS AND OTHER MATTERS
Section 12xx—Three-Year Extension of Authorization for Non-Conventional Assisted Recovery Capabilities
Section 12xx—Limitation on Establishment of Regional Special Operations Forces Coordination Centers

---

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

LEGISLATIVE PROVISIONS

SUBTITLE B—PROGRAM REQUIREMENTS, RESTRICTIONS, AND LIMITATIONS

Section 2xx—Limitation on Availability of Funds for Air Force Logistics Transformation

This section would restrict the obligation and expenditure of Air Force procurement and research, development, test, and evaluation funds for logistics information technology programs until 30 days after the date on which the Secretary of the Air Force submits to the congressional defense committees a report on the modernization and update of Air Force logistics information technology systems following the cancellation of the expeditionary combat support system.

Section 2xx—Limitation on Availability of Funds for Defensive Cyberspace Operations of the Air Force

This section would limit the funds the Air Force may obligate or expend for Defensive Cyberspace Operations in Program Element 0202088F to not more than 90 percent until a period of 30 days after the date on which the Secretary of the Air Force submits a report to the congressional defense committees detailing the Air Force's plan for sustainment of the Application Software Assurance Center of Excellence across the Future Years Defense Program.

Section 2xx—Limitation on the Availability of Funds for the Program Manager for Biometrics of the Department of Defense

This section would restrict the obligation or expenditure of funds for fiscal year 2014 for research, development, test, and evaluation by the Department of Defense program manager for biometrics for future biometric architectures or systems to not more than 75 percent for a period of 30 days after the date on which the Secretary of Defense submits a report to the congressional defense committees assessing the future program structure for biometrics oversight and execution and architectural requirements for biometrics enabling capability.

SUBTITLE E—OTHER MATTERS

Section 2xx—Extension of Authority to Award Prizes for Advanced Technology Achievements

This section would extend the authority of the Department of Defense to award prizes for advanced technology achievements until September 30, 2018.

Section 2xx—Five-Year Extension of Pilot Program to Include Technology Protection Features During Research and Development of Certain Defense Systems

The section would extend the pilot program established by section 243 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111-383), as amended by section 252 of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112-81), from October 1, 2015, to October 1, 2020.

Section 2xx—Establishment of Cryptographic Modernization Review and Advisory Board

This section would require the Secretary of Defense to establish a senior-level body, to be known as the Cryptographic Modernization Review and Advisory Board, to assess and advise the cryptographic modernization activities of the Department of Defense.

TITLE III—OPERATION AND MAINTENANCE

LEGISLATIVE PROVISIONS

SUBTITLE F—LIMITATIONS AND EXTENSIONS OF AUTHORITY

Section 3xx—Revision to Requirement for Annual Submission of Information Regarding Information Technology Capital Assets

This section would would amend the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (Public Law 107-314; 10 U.S.C. 221 note) to align Department of Defense high-threshold information technology Capital Asset reporting with the Department's Major Automated Information Systems reporting and its Exhibit 300 reporting to the Office of Management and Budget.

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

LEGISLATIVE PROVISIONS

SUBTITLE A—ACQUISITION POLICY AND MANAGEMENT

Section 8xx—Modification of Reporting Requirement for Department of Defense Business System Acquisition Programs when Initial Operating Capability is not Achieved within Five-Years of Milestone A Approval

This section would amend the reporting requirement imposed on defense business systems (DBS) acquisition programs by section 811 of the John Warner

National Defense Authorization Act for Fiscal Year 2007 (Public Law 109-364) by clarifying the separate treatment of Major Automated Information Systems (MAIS) DBS and non-MAIS DBS. Specifically, this section would clarify that section 811 is inapplicable to MAIS DBS acquisition programs because such programs are independently subject to critical change reporting under section 2445c of title 10, United States Code. This section would also modify the requirement for non-MAIS DBS reporting a failure to achieve initial operational capacity (IOC) within 5-years of milestone A approval from a critical change report to a report to the Department of Defense pre-certification authority explaining the causes and circumstances surrounding the failure to achieve IOC within the required time.

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

LEGISLATIVE PROVISIONS

SUBTITLE A—DEPARTMENT OF DEFENSE MANAGEMENT

Section 9xx—Revised Definition for Legacy Systems in Defense Business Enterprise Architecture

This section would revise the definition for legacy systems in section 2222 of title 10, United States Code, to those that will be phased out of the defense business enterprise architecture within 3 years after the latest published version of the defense business enterprise architecture.

SUBTITLE C—INTELLIGENCE-RELATED ACTIVITIES

Section 9xx—Department of Defense Intelligence Priorities

This section would require 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. This section would also require the Secretary of Defense to identify any significant intelligence gaps of the Office of the Secretary of Defense, the Joint Staff, the combatant commands, and the military departments. The Secretary would provide a briefing to the congressional defense committees and the congressional intelligence committees regarding the policy established under this section and any identified significant intelligence gaps.

Section 9xx—Defense Clandestine Service

This section would prohibit the use of 50 percent of the funds authorized to be appropriated by this Act or otherwise available to the Department of Defense for fiscal year 2014 for the Defense Clandestine Service to be obligated or expended for the Defense Clandestine Service until such time as the Secretary of Defense certifies 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 that the Defense Clandestine Service is designed primarily to fulfill requirements of the Department of Defense that are unique to the Department of Defense or otherwise unmet; and provide unique capabilities to the intelligence community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

This section would also require the Secretary of Defense to: design metrics that will be used to ensure that the Defense Clandestine Service is employed in the manner certified; provide annual assessments for 5-years based on the metrics established; submit prompt notifications of any significant changes; and provide quarterly briefings on deployments and collection activities.

Section 9xx—Revision of Secretary of Defense Authority to Engage in Commercial Activities as Security for Intelligence Collection Activities

This section would amend current statutory authority for the Secretary of Defense to authorize the conduct of those commercial activities necessary to provide security for authorized intelligence collection activities abroad undertaken by the Department of Defense. This section would:

(1) Delete the requirement that the Secretary of Defense designate a single office within the Defense Intelligence Agency to be responsible for the management and supervision of all commercial activities authorized by the intelligence commercial activity statute (10 U.S.C. 431-437);

(2) Change the annual audit requirement to a biennial audit requirement;

(3) Add the congressional defense committees to the reporting requirement; and

(4) Insert a definition of “congressional intelligence committees” for purposes of section 437 of title 10, United States Code.

SUBTITLE E—CYBERSPACE-RELATED MATTERS

Section 9xx—Mission Analysis for Cyber Operations of Department of Defense

This section would require the Secretary of Defense to conduct a mission analysis of Department of Defense cyber operations and to provide a report on the results of the mission analysis to the congressional defense committees.

The committee notes that the Defense Science Board recently completed a report titled "Resilient Military Systems and the Advanced Cyber Threat." In particular, the committee recognizes the need to address a key recommendation in

the report that would require the Department to determine the mix of cyber, protected-conventional, and nuclear capabilities necessary for assured operation in the face of a full-spectrum adversary by designating a mix of forces necessary to conduct assured operations, including systems such as penetrating bombers, submarines with long range cruise missiles, Conventional Prompt Global Strike (CPGS), and survivable senior leadership command and control. The committee believes the Department will need to address this recommendation as it conducts the mission analysis required by this section.

In addition, the committee is aware that there is interest from the Department as well as Congress on how best to leverage the Reserve Component, including the National Guard, in the Department's organizing construct for cyber operations. While the committee supports these considerations, it is also concerned that current legislative proposals to dictate National Guard units for each of the states and territories is premature and may be detrimental to the overall national effort. In addition to the hefty price tag, which is estimated to be about $400.0 million per year, current proposals only address National Guard participation and do not include the Reserve Component. Whereas only the Army and the Air Force have National Guard units, all of the military services have Reserve Components that have unique authorities and capabilities that should be addressed by the national effort. The committee believes that more time is needed to evaluate full participation of the Reserve Components, including the implications and limitations of using National Guard forces in a "title 32" capacity, before broader action is take. The committee encourages the Department to examine these issues in the course of the mission analysis required by this section.

TITLE X—GENERAL PROVISIONS

LEGISLATIVE PROVISIONS

SUBTITLE D—COUNTERTERRORISM

Section 10xx—Modification of Regional Defense Combating Terrorism Fellowship Program Reporting Requirement

This section would modify the Regional Defense Combating Terrorism Fellowship Program to require additional annual reporting requirements.

SUBTITLE F—STUDIES AND REPORTS

Section 10xx—Strategy for Future Military Information Operations Capabilities

This section would require the Secretary of Defense to develop and implement a strategy for developing and sustaining military information operations

capabilities for future contingencies. This strategy would be delivered to the congressional defense committees by February 1, 2014.

SUBTITLE H—OTHER MATTERS

Section 10xx—Reduction in Costs to Report Critical Changes to Major Automated Information System Programs

This section would give Department of Defense senior officials responsible for major automated information system programs the option of submitting to the congressional defense committees either a critical change report when required, or a streamlined notification when the official further concludes that the critical change occurred primarily due to congressional action, such as a reduction in program funding.

Section 10xx—Enhancement of Capacity of the United States Government to Analyze Captured Records

This section would allow the Secretary of Defense to establish a Conflict Records Research Center to facilitate research and analysis of records captured from countries, organizations, and individuals, now or once hostile, to the United States.

The committee recognizes that there are significant records available to the U.S. Government that could be useful for academic and policy research once immediate, tactical exploitation and dissemination has occurred. The committee believes that research and analysis of such captured records would increase the understanding of factors related to international relations, counterterrorism, conventional and unconventional warfare and, ultimately, enhance national security.

The committee notes that such a center currently exists, but additional statutory authorization would allow the Center to be funded collectively by the Department of Defense and the Office of the Director of National Intelligence, and other departments and agencies, rather than rely on discrete partner funding for each activity. This would also allow the Center to receive funding from other agencies, states, or other foreign and domestic entities.

The committee also understands that there exists procedures by which the intelligence community works with this Center to ensure that the intelligence value of specific documents is exhausted before releasing them to the academic community, as well as ensure the protection of classified information, sources and methods, and personally identifiable information. The committee expects the Center to ensure such procedures continue to be implemented in a manner to protect such information and encourages the Department to continue working with the Office of the Director of National Intelligence to refine and improve those procedures.

Section 10xx—Review and Assessment of United States Special Operations Forces and United States Special Operations Command

This section would require the Secretary of Defense of the United States to review and assess the organization, missions, and authorities related to U.S. Special Operations Forces and U.S. Special Operations Command and to provide a report to the congressional defense committees.

Section 10xx—Inclusion in Annual Report of Description of Interagency Coordination relating to Humanitarian Demining Technology

This section would modify current reporting requirements for humanitarian demining as defined within in section 407(d) of title 10, United States Code, to include interagency, research and development activities.

Section 10xx—Protection of Tier One Task Critical Assets from Electromagnetic Pulse and High-Powered Microwave Systems

This section would require the Secretary of Defense to certify to the congressional defense committees that defense critical assets designated as tier one task critical assets (TCAs) are protected from the adverse effects of electromagnetic pulses and high-powered microwave systems. For tier one TCAs not certified, the Department shall submit a plan on how to mitigate any risks to mission assurance, including any steps that may be needed for remediation.

TITLE XI—CIVILIAN PERSONNEL MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE A—GENERAL PROVISIONS

Section 11xx—Extension of Program for Exchange of Information-Technology Personnel

This section would remove the sunset date for this program, and permanently establish the Information Technology Exchange Program (ITEP) for the Department of Defense.

The committee is aware that ITEP was established in order to allow employees from the private sector or academia to temporarily work for the Department of Defense, as well as Department of Defense employees to work in the private sector. The committee believes that this kind of technical exchange of ideas is helpful in fostering the sharing of industry, federal cultures, and technical expertise in ways that will help modernize the Department of Defense by exposing its employees to best practices from the constantly changing and evolving informational technology sector, especially in key areas like cloud computing, cyber

security, information technology (IT) consolidation, network services, IT project and data management, and enterprise architecture. The committee also believes industry will benefit from learning how the Department of Defense operates and how it can better serve the Department's needs.

Section 11xx—Revision to Amount of Financial Assistance under Department of Defense Science, Mathematics, and Research for Transformation (SMART) Defense Education Program

This section would remove the specific items for which financial assistance may be provided under the Science, Mathematics, and Research for Transformation (SMART) program. Such revisions would increase the flexibility that the Secretary of Defense would have in exercising discretion in administration of the SMART Program and will lessen the administrative burden in SMART Program operations. It would also allow the Secretary to make SMART Program stipend costs more consistent with other Federal scholarship-for-service educational programs.

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

LEGISLATIVE PROVISIONS

SUBTITLE __—MATTERS RELATING TO AFGHANISTAN POST 2014

Section 12xx—Defense Intelligence Plan

This section would require the Secretary of Defense to submit to the congressional defense committees and the congressional intelligence committees a Department of Defense plan regarding covered defense intelligence assets in relation to the drawdown of U.S. forces in the Islamic Republic of Afghanistan. This section would require the plan to include:

(1) A description of the covered defense intelligence assets;

(2) A description of any such assets to remain in Afghanistan after December 31, 2014;

(3) A description of any such assets that will be, or have been, reallocated to other locations outside of the United States;

(4) The defense intelligence priorities that will be, or have been, addressed with the reallocation of such assets;

(5) The necessary logistics, operations, and maintenance plans to operate in the locations where such assets, including personnel, basing, and any host country agreements, will be, or have been, reallocated; and

(6) A description of any such assets that will be, or have been, returned to the United States.

Further discussion is contained in the classified annex accompanying this report.

SUBTITLE D—REPORTS AND OTHER MATTERS

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

This section would authorize the Department of Defense a 3-year extension to continue to develop, manage, and execute a Non-Conventional Assisted Recovery personnel recovery program for isolated Department of Defense, U.S. Government, and other designated personnel supporting U.S. national interests globally. This section would allow the Secretary of Defense to use funds through fiscal year 2017.

Section 12xx—Limitation on Establishment of Regional Special Operations Forces Coordination Centers

This section would limit the expenditure of funds for the establishment of "Regional Special Operations Forces Coordination Centers" or similar regional entities. This section would also require a joint report by the Secretary of Defense and the Secretary of State to be submitted to the congressional defense committees and the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

BILL LANGUAGE

SEC. 2____. [Log 50314] LIMITATION ON AVAILABILITY OF FUNDS FOR AIR FORCE LOGISTICS TRANSFORMATION.

Of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2014 for procurement, Air Force, or research, development, test, and evaluation, Air Force, for logistics information technology, including for the expeditionary combat support system, not more than 50 percent may be obligated or expended until the date that is 30 days after the date on which the Secretary of the Air Force submits to the congressional defense committees a report on how the Secretary will modernize and update the logistics information technology systems of the Air Force following the cancellation of the expeditionary combat support system. Such report shall include—

(1) strategies to—

(A) in the near term, address any gaps in capability with respect to logistics information technology; and

(B) during the period covered by the current future-years defense plan, provide for long-term modernization of logistics information technology;

(2) an analysis of the root causes leading to the failure of the expeditionary combat support system program; and

(3) a plan of action by the Secretary to ensure that the lessons learned under such analysis are—

(A) shared throughout the Department of Defense and the military departments; and

(B) considered in program planning for similar logistics information technology systems.

SEC. 2____. [Log 50882] LIMITATION ON AVAILABILITY OF FUNDS FOR DEFENSIVE CYBERSPACE OPERATIONS OF THE AIR FORCE.

(a) LIMITATION.— Of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2014 for procurement, Air Force, or research, development, test, and evaluation, Air Force, for Defensive Cyberspace Operations (Program Element 0202088F), not more than 90 percent may be obligated or expended until a period of 30 days has elapsed following the date on which the Secretary of the Air Force submits to the congressional defense committees a report on the Application Software Assurance Center of Excellence.

(b) MATTERS INCLUDED.—The report under subsection (a) shall include the following:

(1) A description of how the Application Software Assurance Center of Excellence is used to support the software assurance activities of the Air Force and other elements of the Department of Defense, including pursuant to section 933 of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239; 10 U.S.C. 2224 note).

(2) A description of the resources used to support the Center of Excellence from the beginning of the Center through fiscal year 2014.

(3) The plan of the Secretary for sustaining the Center of Excellence during the period covered by the future-years defense program submitted in 2013 under section 221 of title 10, United States Code.

SEC. 2___. [Log 50962] LIMITATION ON AVAILABILITY OF FUNDS FOR THE PROGRAM MANAGER FOR BIOMETRICS OF THE DEPARTMENT OF DEFENSE.

(a) LIMITATION.— Of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2014 for research, development, test, and evaluation for the Department of Defense program manager for biometrics for future biometric architectures or systems, not more than 75 percent may be obligated or expended until a period of 30 days has elapsed following the date on which the Secretary of Defense submits to the congressional defense committees a report assessing the future program structure for biometrics oversight and execution and architectural requirements for biometrics enabling capability.

(b) MATTERS INCLUDED.—The report under subsection (a) shall include the following:

(1) An assessment of the roles and responsibilities of the principal staff assistant for biometrics, the program manager for biometrics, and the Biometrics Identity Management Agency, including an analysis of alternatives to evaluate—

(A) how to better align responsibilities for the multiple elements of the military departments and the Department of Defense with responsibility for biometrics, including the Navy and the Marine Corps; the Office of the Provost Marshall General, and the intelligence community; and

(B) whether the program management responsibilities of the Department of Defense program manager for biometrics should be retained by the Army or transferred to another military department or element of the Department based on the expected future operating environment.

(2) An assessment of the current requirements for the biometrics enabling capability to ensure the capability continues to meet the needs of the relevant military departments and elements of the Department of Defense based on the future operating environment after the drawdown in Afghanistan.

(3) An analysis of the need to merge the program management structures and systems architecture and requirements development process for biometrics and forensics applications.

SEC. 2____. [Log 50315] EXTENSION OF AUTHORITY TO AWARD PRIZES FOR ADVANCED TECHNOLOGY ACHIEVEMENTS.

Section 2374a(f) of chapter 139 of title 10, United States Code, is amended by striking ''September 30, 2013'' and inserting ''September 30, 2018''.

SEC. 2____. [Log 50738] FIVE-YEAR EXTENSION OF PILOT PROGRAM TO INCLUDE TECHNOLOGY PROTECTION FEATURES DURING RESEARCH AND DEVELOPMENT OF CERTAIN DEFENSE SYSTEMS.

Section 243(d) of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383; 10 U.S.C. 2358 note) is amended by striking ''October 1, 2015'' and inserting ''October 1, 2020''.

SEC. 2___. [Log 50778] ESTABLISHMENT OF CRYPTOGRAPHIC MODERNIZATION OVERSIGHT AND ADVISORY BOARD.

(a) IN GENERAL.—Chapter 7 of title 10, United States Code, is amended by adding at the end the following new section:

"§ 189. Cryptographic Modernization Oversight and Advisory Board

''(a) ESTABLISHMENT.—There shall be in the Department of Defense a Cryptographic Modernization Oversight and Advisory Board (in this section referred to as the 'Board') to oversee the cryptographic modernization activities of the Department and provide advice to the Secretary with respect to such activities.

''(b) MEMBERS.—(1) The Secretary shall determine the number of members of the Board.

''(2) The Secretary shall appoint officers in the grade of general or admiral and civilian employees of the Department of Defense in the Senior Executive Service to serve as members of the Board.

''(c) RESPONSIBILITIES.—The Board shall—

''(1) review the cease-use dates for specific cryptographic systems based on rigorous analysis of technical and threat factors and issue guidance, as

needed, to relevant program executive offices and program managers;

"(2) monitor the overall cryptographic modernization efforts of the Department, including while such efforts are being executed;

"(3) convene in-depth technical program reviews, as needed, for specific cryptographic modernization developments with respect to validating current and in-draft requirements and identifying programmatic risks;

"(4) develop a five-year cryptographic modernization plan to—

"(A) revalidate requirements previously approved by the Joint Requirements Oversight Council with respect to cryptographic modernization; and

"(B) identify previously unidentified requirements;

"(5) develop a long-term roadmap to—

"(A) ensure synchronization with major planning documents;

"(B) anticipate risks and issues in 10- and 20-year timelines; and

"(C) ensure that the expertise and insights of the military departments, Defense Agencies,

the combatant commands, industry, academia, and key allies are included in the course of developing and carrying out cryptographic modernization activities;

''(6) develop a concept of operations for how cryptographic systems should function in a system-of-systems environment; and

''(7) advise the Secretary on the development of a cryptographic asset visibility system.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended by adding after the item relating to section 188 the following new item:

''189. Cryptographic Modernization Oversight and Advisory Board.''.

SEC. 3___[Log 50735]. REVISION TO REQUIREMENT FOR ANNUAL SUBMISSION OF INFORMATION REGARDING INFORMATION TECHNOLOGY CAPITAL ASSETS.

Section 351(a)(1) of the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (Public Law 107-314; 10 U.S.C. 221 note) is amended by striking ''in excess of $30,000,000'' and all that follows and inserting ''(as computed in fiscal year 2000 constant dollars) in excess of $32,000,000 or an estimated total cost for the future-years defense program for which the budget is submitted (as computed in fiscal year 2000 constant dollars) in excess of $378,000,000, for all expenditures, for all increments, regardless of the appropriation and fund source, directly related to the assets definition, design, development, deployment, sustainment, and disposal.''.

SEC. 8____ [Log 50734]. MODIFICATION OF REPORTING REQUIREMENT FOR DEPARTMENT OF DEFENSE BUSINESS SYSTEM ACQUISITION PROGRAMS WHEN INITIAL OPERATING CAPABILITY IS NOT ACHIEVED WITHIN FIVE YEARS OF MILESTONE A APPROVAL.

(a) SUBMISSION TO PRE-CERTIFICATION AUTHORITY.—Subsection (b) of section 811 of the John Warner National Defense Authorization Act for Fiscal Year 2007 (Public Law 109-364; 120 Stat. 2316; 10 U.S.C. 2222 note) is amended by striking ''the system shall be deemed to have undergone'' and all that follows through the period and inserting ''the appropriate official shall report such failure, along with the facts and circumstances surrounding the failure, to the appropriate pre-certification authority for that system under section 2222 of title 10, United States Code, and the information so reported shall be considered by the pre-certification authority in the decision whether to recommend certification of obligations under that section.''.

(b) COVERED SYSTEMS.—Subsection (c) of such section is amended—

(1) by striking ''3542(b)(2) of title 44'' and inserting ''section 2222(j)(2) of title 10''; and

(2) by inserting ", and that is not designated in section 2445a of title 10, United States Code, as a 'major automated information system program' or an 'other major information technology investment program'" before the period at the end.

(c) UPDATED REFERENCES TO DOD ISSUANCES.—Subsection (d) of such section is amended—

(1) in paragraph (1), by striking "Department of Defense Instruction 5000.2" and inserting "Department of Defense Directive 5000.01"; and

(2) in paragraph (2), by striking "Department of Defense Instruction 5000.2, dated May 12, 2003" and inserting "Department of Defense Instruction 5000.02, dated December 3, 2008".

SEC. 9____ [Log 50874]. REVISED DEFINITION FOR LEGACY SYSTEMS IN DEFENSE BUSINESS ENTERPRISE ARCHITECTURE.

Section 2222(e)(2) of title 10, United States Code, is amended by striking ''existing as of September 30, 2011 (known as 'legacy systems') that will not be part of the defense business enterprise architecture'' and inserting ''that will be phased out of the defense business enterprise architecture within three years after the latest published version of the defense business enterprise architecture (known as 'legacy systems')''.

SEC. [9____ Log 50451]. DEPARTMENT OF DEFENSE INTELLIGENCE PRIORITIES.

Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall—

(1) 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;

(2) identify any significant intelligence gaps of the Office of the Secretary of Defense, the Joint Staff, the combatant commands, and the military departments; and

(3) 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 the policy established under paragraph (1) and the gaps identified under paragraph (2).

SEC. [9___ Log 50951]. DEFENSE CLANDESTINE SERVICE.

(a) CERTIFICATION REQUIRED.—Not more than 50 percent of the funds authorized to be appropriated by this Act or otherwise available to the Department of Defense for the Defense Clandestine Service for fiscal year 2014 may be obligated or expended for the Defense Clandestine Service until such time as the Secretary of Defense certifies to the covered congressional committees that—

(1) the Defense Clandestine Service is designed primarily to—

(A) fulfill priorities of the Department of Defense that are unique to the Department of Defense or otherwise unmet; and

(B) provide unique capabilities to the intelligence community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))); and

(2) the Secretary of Defense has designed metrics that will be used to ensure that the Defense Clandestine Service is employed as described in paragraph (1).

(b) ANNUAL ASSESSMENTS.—Not later than 120 days after the date of the enactment of this Act, and annually thereafter for five years, the Secretary of Defense

shall submit to the covered congressional committees a detailed assessment of Defense Clandestine Service employment and performance based on the metrics referred to in subsection (a)(2).

(c) NOTIFICATION OF FUTURE CHANGES TO DESIGN.—Following the submittal of the certification referred to in subsection (a), in the event that any significant change is made to the Defense Clandestine Service, the Secretary shall promptly notify the covered congressional committees of the nature of such change.

(d) QUARTERLY BRIEFINGS.—The Secretary of Defense shall quarterly provide to the covered congressional committees a briefing on the deployments and collection activities of personnel of the Defense Clandestine Service.

(e) COVERED CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''covered congressional committees'' 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.

SEC. [9___ Log 51058]. REVISION OF SECRETARY OF DEFENSE AUTHORITY TO ENGAGE IN COMMERCIAL ACTIVITIES AS SECURITY FOR INTELLIGENCE COLLECTION ACTIVITIES.

(a) PERIOD FOR REQUIRED AUDITS.—Section 432(b)(2) of title 10, United States Code, is amended—

(1) in the first sentence, by striking ''annually'' and inserting ''biennially''; and

(2) in the second sentence, by striking ''the intelligence committees'' and all that follows and inserting ''the congressional defense committees and the congressional intelligence committees (as defined in section 437(c)).''

(b) REPEAL OF DESIGNATION OF DEFENSE INTELLIGENCE AGENCY AS REQUIRED OVERSIGHT AUTHORITY WITHIN DEPARTMENT OF DEFENSE.—Section 436(4) of title 10, United States Code, is amended—

(1) by striking ''Defense Intelligence Agency'' and inserting ''Department of Defense''; and

(2) by striking ''management and supervision'' and inserting ''oversight''.

(c) CONGRESSIONAL OVERSIGHT.—Section 437 of title 10, United States Code, is amended—

(1) in subsection (a), by striking ''the intelligence committees'' and inserting ''congressional defense committees and the congressional intelligence committees'';

(2) in subsection (b), by striking ''the intelligence committees'' and inserting ''congressional defense committees and the congressional intelligence committees''; and

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

''(c) CONGRESSIONAL INTELLIGENCE COMMITTEES DEFINED.—In this section, the term 'congressional intelligence committees' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).''.

SEC. 9____. [Log 51000] MISSION ANALYSIS FOR CYBER OPERATIONS OF DEPARTMENT OF DEFENSE.

(a) MISSION ANALYSIS REQUIRED.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall conduct a mission analysis of the cyber operations of the Department of Defense.

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

(1) The concept of operations and concept of employment for cyber operations forces.

(2) An assessment of the manpower needs for cyber operations forces, including military requirements for both active and reserve components and civilian requirements.

(3) A description of the alignment of the organization and reporting chains of the Department, the military departments, and the combatant commands.

(4) An assessment of the current, as of the date of the analysis, and projected equipping needs of cyber operations forces.

(5) An analysis of how the Secretary, for purposes of cyber operations, depends upon organiza-

tions outside of the Department, including industry and international partners.

(6) Methods for ensuring resilience, mission assurance, and continuity of operations for cyber operations.

(c) REPORT REQUIRED.—Not later than 30 days after the completion of the mission analysis under subsection (a), the Secretary shall submit to the congressional defense committees a report containing—

(1) the results of the mission analysis; and

(2) recommendations for improving or changing the roles, organization, missions, concept of operations, or authorities related to the cyber operations of the Department.

(d) FORM.—The report under subsection (c) shall be submitted in unclassified form, but may include a classified annex.

SEC. 10___[Log 50853]. MODIFICATION OF REGIONAL DEFENSE COMBATING TERRORISM FELLOWSHIP PROGRAM REPORTING REQUIREMENT.

(a) IN GENERAL.—Section 2249c(c) of title 10, United States Code, is amended—

(1) in paragraph (3), by inserting ", including engagement activities for program alumni," after "effectiveness of the program";

(2) in paragraph (4), by inserting after "program" the following: ", including a list of any unfunded or unmet training requirements and requests"; and

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

"(5) A discussion and justification of how the program fits within the theater security priorities of each of the commanders of the geographic combatant commands.".

(b) EFFECTIVE DATE.—The amendments made by subsection (a) shall apply with respect to a report submitted for a fiscal year beginning after the date of the enactment of this Act.

SEC. 10___[Log 50777]. STRATEGY FOR FUTURE MILITARY INFORMATION OPERATIONS CAPABILITIES.

(a) STRATEGY REQUIRED.—The Secretary of Defense shall develop and implement a strategy for developing and sustaining military information operations capabilities for future contingencies. The Secretary shall submit such strategy to the congressional defense committees by not later than February 1, 2014.

(b) CONTENTS OF STRATEGY.—The strategy required in subsection (a) shall include each of the following:

(1) A plan for the sustainment of existing capabilities that have been developed during the ten-year period prior to the date of the enactment of this Act, including such capabilities developed using funds authorized to be appropriated for overseas contingency operations.

(2) A discussion of how the capabilities referred to in paragraph (1) are being integrated into both operational plans (OPLANS) and contingency plans (CONPLANS).

(3) An assessment of the force structure that is necessary to support operational planning and potential contingency operations, including the relative balance across the active and reserve components.

(4) Estimates of the steady-state resources needed to support the force structure referred to in paragraph (3), as well as estimates for resources that might be needed based on selected OPLANS and CONPLANS.

(5) A description of how new and emerging technologies can be incorporated into the projected force structure and future OPLANS and CONPLANS.

(6) A description of new capabilities that may be needed to fill any identified gaps and programs that might be required to develop such capabilities.

SEC. 10___[Log 50737]. 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 CONGRESSIONAL ACTION OR EXTENSION OF PROGRAM.—If a senior Department of Defense official 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) either (A) are primarily the result of congressional action, or (B) 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 those determinations. 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. 10___[Log 50700]. ENHANCEMENT OF CAPACITY OF THE UNITED STATES GOVERNMENT TO ANALYZE CAPTURED RECORDS.

(a) IN GENERAL.—Chapter 21 of title 10, United States Code, is amended by inserting after section 426 the following new section:

"§ 427. Conflict Records Research Center

''(a) CENTER AUTHORIZED.—The Secretary of Defense may establish a center to be known as the 'Conflict Records Research Center' (in this section referred to as the 'Center').

''(b) PURPOSES.—The purposes of the Center shall be the following:

''(1) To establish a digital research database including translations and to facilitate research and analysis of records captured from countries, organizations, and individuals, now or once hostile to the United States, with rigid adherence to academic freedom and integrity.

''(2) To make a significant portion of these records available to researchers as quickly and responsibly as possible while taking into account legitimate national security concerns, the integrity of the

academic process, and risks to innocents or third parties.

"(3) To conduct and disseminate research and analysis to increase the understanding of factors related to international relations, counterterrorism, and conventional and unconventional warfare and, ultimately, enhance national security.

"(4) To collaborate with members of academic and broad national security communities, both domestic and international, on research, conferences, seminars, and other information exchanges to identify topics of importance for the leadership of the United States Government and the scholarly community.

"(c) CONCURRENCE OF THE DIRECTOR OF NATIONAL INTELLIGENCE.—The Secretary of Defense shall seek the concurrence of the Director of National Intelligence to the extent the efforts and activities of the Center involve the entities referred to in subsection (b)(4).

"(d) SUPPORT FROM OTHER UNITED STATES GOVERNMENT DEPARTMENTS OR AGENCIES.—The head of any non-Department of Defense department or agency of the United States Government may—

"(1) provide to the Secretary of Defense services, including personnel support, to support the operations of the Center; and

"(2) transfer funds to the Secretary of Defense to support the operations of the Center.

"(e) ACCEPTANCE OF GIFTS AND DONATIONS.—(1) Subject to paragraph (3), the Secretary of Defense may accept from any source specified in paragraph (2) any gift or donation for purposes of defraying the costs or enhancing the operations of the Center.

"(2) The sources specified in this paragraph are the following:

"(A) The government of a State or a political subdivision of a State.

"(B) The government of a foreign country.

"(C) A foundation or other charitable organization, including a foundation or charitable organization that is organized or operates under the laws of a foreign country.

"(D) Any source in the private sector of the United States or a foreign country.

"(3) The Secretary may not accept a gift or donation under this subsection if acceptance of the gift or donation would compromise or appear to compromise—

"(A) the ability of the Department of Defense, any employee of the Department, or any member of the armed forces to carry out the responsibility or duty of the Department in a fair and objective manner; or

"(B) the integrity of any program of the Department or of any person involved in such a program.

"(4) The Secretary shall provide written guidance setting forth the criteria to be used in determining the applicability of paragraph (3) to any proposed gift or donation under this subsection.

"(f) CREDITING OF FUNDS TRANSFERRED OR ACCEPTED.—Funds transferred to or accepted by the Secretary of Defense under this section shall be credited to appropriations available to the Department of Defense for the Center, and shall be available for the same purposes, and subject to the same conditions and limitations, as the appropriations with which merged. Any funds so transferred or accepted shall remain available until expended.

"(g) DEFINITIONS.—In this section:

"(1) The term 'captured record' means a document, audio file, video file, or other material captured during combat operations from countries, or-

ganizations, or individuals, now or once hostile to the United States.

"(2) The term 'gift or donation' means any gift or donation of funds, materials (including research materials), real or personal property, or services (including lecture services and faculty services).".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of subchapter I of such chapter is amended by inserting after the item relating to section 426 the following new item:

"427. Conflict Records Research Center.".

SEC. 10___[Log 50976]. REVIEW AND ASSESSMENT OF UNITED STATES SPECIAL OPERATIONS FORCES AND UNITED STATES SPECIAL OPERATIONS COMMAND.

(a) IN GENERAL.—The Secretary of Defense shall conduct a review of the United States Special Operations Forces organization, capabilities, and structure.

(b) REPORT.—Not later than the date on which the budget of the President is submitted to Congress under section 1105(a) of title 31, United States Code, for fiscal year 2015, the Secretary of Defense shall submit to the congressional defense committees a report on the review conducted under subsection (a). Such report shall include an analysis of each of the following:

(1) The organizational structure of the United States Special Operations Command and each subordinate component, as in effect as of the date of the enactment of this Act.

(2) The policy and civilian oversight structures for Special Operations Forces within the Department of Defense, as in effect as of the date of the enactment of this Act, including the statutory structures and responsibilities of the Office of the Sec-

retary of Defense for Special Operations and Low Intensity Conflict within the Department.

(3) The roles and responsibilities of United States Special Operations Command and Special Operations Forces under section 167 of title 10, United States Code.

(4) Current and future special operations peculiar requirements of the commanders of the geographic combatant commands, Theater Special Operations Commands, and command relationships between United States Special Operations Command and the geographic combatant commands.

(5) The funding authorities, uses, and oversight mechanisms of Major Force Program–11.

(6) Changes to structure, authorities, oversight mechanisms, Major Force Program–11 funding, roles, and responsibilities assumed in the 2014 Quadrennial Defense Review.

(7) Any other matters the Secretary of Defense determines are appropriate to ensure a comprehensive review and assessment.

(c) IN GENERAL.—Not later than 60 days after the date on which the report required by subsection (b) is submitted, the Comptroller General of the United States shall submit to the congressional defense committees a review

of the report. Such review shall include an assessment of United States Special Operations Forces organization, capabilities, and force structure with respect to conventional force structures and national military strategies.

SEC. 10___[Log 50133]. INCLUSION IN ANNUAL REPORT OF DESCRIPTION OF INTERAGENCY COORDINATION RELATING TO HUMANITARIAN DEMINING TECHNOLOGY.

Section 407(d) of title 10, United States Code, is amended—

(1) in paragraph (3), by striking ''and'' at the end;

(2) in paragraph (4), by striking the period and inserting ''; and''; and

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

''(5) a description of interagency efforts to coordinate and improve research, development, test, and evaluation for humanitarian demining technology and mechanical clearance methods, including the transfer of relevant counter-improvised explosive device technology with potential humanitarian demining applications.''.

SEC. 10___[Log 51057]. PROTECTION OF TIER ONE TASK CRITICAL ASSETS FROM ELECTROMAGNETIC PULSE AND HIGH-POWERED MICROWAVE SYSTEMS.

(a) CERTIFICATION REQUIRED.—Not later than June 1, 2014, the Secretary of the Defense shall submit to the congressional defense committees certification that defense critical assets designated as tier one task critical assets (hereinafter referred to as ''TCAs'') are protected from the adverse effects of man-made or naturally occurring electromagnetic pulse and high-powered microwave weapons. Any such assets found not to be so protected shall be included in the plan required under subsection (b).

(b) PLAN REQUIRED.—Not later than January 1, 2015, the Secretary of the Defense shall submit to the congressional defense committees a plan for tier one TCAs to receive electricity by means that are protected from the adverse effects of man-made or naturally occurring electromagnetic pulse and high-powered microwave weapons. The plan shall include the following elements:

(1) An analysis of how the Department of Defense plans to mitigate any risks to mission assurance for non-certified tier one TCAs, including any steps that may be needed for remediation.

(2) The development or adoption by the Department of a standard of resistance or protection against man-made and natural electromagnetic threats for electricity sources that supply electricity to tier one TCAs.

(3) The development by the Department of a strategy to certify by December 31, 2015, that all electricity sourced to tier one TCAs is provided by facilities that meet the standard developed under paragraph (2).

(c) PREPARATION OF PLAN.—In preparing the plan required by subsection (b), the Secretary of Defense shall use the guidance and recommendations of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack established by section 1401 of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (as enacted into law by Public Law 106–398; 114. Stat. 1654A–345).

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

(e) DEFINITIONS.—In this section:

(1) The term ''task critical asset'' means an asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a debilitating effect on the

ability of the Department of Defense to fulfill its missions.

(2) The term ''tier one'' with respect to a task critical asset means such an asset the loss, incapacitation, or disruption of which could result in mission (or function) failure at the Department of Defense, military department, combatant command, sub-unified command, Defense Agency, or defense infrastructure sector level.

SEC. 11___ [Log 50407]. EXTENSION OF PROGRAM FOR EXCHANGE OF INFORMATION-TECHNOLOGY PERSONNEL.

(a) IN GENERAL.—Section 1110(d) of the National Defense Authorization Act for Fiscal Year 2010 (5 U.S.C. 3702 note) is amended by striking ''2013.'' and inserting ''2023.''.

(b) REPORTING REQUIREMENT.—Section 1110(i) of such Act is amended by striking ''2015,'' and inserting ''2024,''.

SEC. 11____ [Log 50862]. REVISION TO AMOUNT OF FINANCIAL ASSISTANCE UNDER DEPARTMENT OF DEFENSE SCIENCE, MATHEMATICS, AND RESEARCH FOR TRANSFORMATION (SMART) DEFENSE EDUCATION PROGRAM.

Paragraph (2) of section 2192a(b) of title 10, United States Code, is amended by striking ''the amount determined'' and all that follows through ''room and board'' and inserting ''an amount determined by the Secretary of Defense''.

SEC. 12__ [Log 50626]. DEFENSE INTELLIGENCE PLAN.

(a) PLAN REQUIRED.—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, the Permanent Select Committee on Intelligence of the House of Representatives, and the Select Committee on Intelligence of the Senate a Department of Defense plan regarding covered defense intelligence assets in relation to the drawdown of the United States Armed Forces in Afghanistan. Such plan shall include—

(1) a description of the covered defense intelligence assets;

(2) a description of any such assets to remain in Afghanistan after December 31, 2014, to continue to support military operations;

(3) a description of any such assets that will be or have been reallocated to other locations outside of the United States in support of the Department of Defense;

(4) the defense intelligence priorities that will be or have been addressed with the reallocation of such assets from Afghanistan;

(5) the necessary logistics, operations, and maintenance plans to operate in the locations where

1 such assets will be or have been reallocated, includ-
2 ing personnel, basing, and any host country agree-
3 ments; and
4 (6) a description of any such assets that will be
5 or have been returned to the United States.
6 (b) COVERED DEFENSE INTELLIGENCE ASSETS DE-
7 FINED.—In this section, the term ''covered defense intel-
8 ligence assets'' means Department of Defense intelligence
9 assets and personnel supporting military operations in Af-
10 ghanistan at any time during the one-year period ending
11 on the date of the enactment of this Act.

SEC. 12___ [Log 50416]. THREE-YEAR EXTENSION OF AUTHORIZATION FOR NON-CONVENTIONAL ASSISTED RECOVERY CAPABILITIES.

Section 943(h) of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110–417; 122 Stat. 4579), as amended by section 1205(g) of the National Defense Authorization Act for Fiscal Year 2012 (Public Law 112–81; 125 Stat. 1624), is further amended by striking ''2013'' and inserting ''2016''.

SEC. 12__ [Log 50922]. LIMITATION ON ESTABLISHMENT OF REGIONAL SPECIAL OPERATIONS FORCES COORDINATION CENTERS.

(a) LIMITATION.—None of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2014 for the Department of Defense may be obligated or expended to plan, prepare, establish, or implement any ''Regional Special Operations Forces Coordination Center'' (RSCC) or similar regional coordination entities.

(b) EXCLUSION.—The limitation contained in subsection (a) shall not apply with respect to any RSCC or similar regional coordination entity authorized by statute, including the North Atlantic Treaty Organization Special Operations Headquarters authorized under section 1244 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84; 123 Stat. 2541).

(c) REPORT.—Not later than 180 days after the date of enactment of this Act, the Secretary of Defense, in coordination with the Secretary of State, shall submit to the congressional committees specified in subsection (d) a report on the following:

(1) A detailed description of the intent and purpose of the RSCC concept.

(2) Defined and validated requirements justifying the establishment of RSCCs or similar entities within each geographic combatant command, to include how such centers have been coordinated and de-conflicted with existing regional and multilateral frameworks or approaches.

(3) An explanation of why existing regional centers and multilateral frameworks cannot satisfy the requirements and needs of the Department of Defense and geographic combatant commands.

(4) Cost estimates across the Future Years Defense Program for such centers, to include estimates of contributions of nations participating in such centers.

(5) Any other matters that the Secretary of Defense or Secretary of State determines appropriate.

(d) SPECIFIED CONGRESSIONAL COMMITTEES.—The congressional committees referred to in subsection (c) are—

(1) the congressional defense committees; and

(2) the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

DIRECTIVE REPORT LANGUAGE

Table Of Contents

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS
TITLE I—PROCUREMENT
OTHER PROCUREMENT, ARMY
Items of Special Interest
Civil Support Team information management needs
TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION
RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, ARMY
Items of Special Interest
Army directed energy testing
RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, NAVY
Items of Special Interest
Maritime Laser Weapon System
RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, DEFENSE-WIDE
Items of Special Interest
Detection and threat identification technologies
Distributed Common Ground System enterprise
Foreign directed energy threats to U.S. military systems
Standardization of directed energy weapon systems characterization
OPERATIONAL TEST AND EVALUATION, DEFENSE
Items of Special Interest
Test and evaluation capabilities for electromagnetic pulse vulnerabilities
TITLE V—MILITARY PERSONNEL POLICY
ITEMS OF SPECIAL INTEREST
U.S. Special Operations Command Educational Initiatives
TITLE VIII—ACQUISITION POLICY, ACQUISITION MANAGEMENT, AND RELATED MATTERS
ITEMS OF SPECIAL INTEREST
Advanced Technical Exploitation Program
Competition in Air Force Network-Centric Solutions Contracts
TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT
ITEMS OF SPECIAL INTEREST
Assessment of Cyber Centers of Academic Excellence
Coordination of Cyber and Electronic Warfare Capabilities
Cyber Standards Framework
Defense Intelligence Collection Management
Input into National Intelligence Priorities Framework
Integrated Science and Technology Campus for the Defense Intelligence Agency
Open-Source Intelligence Utilization

Pilot to Counter Brokers of Transnational Criminal Organizations
Science and Technology Community Intelligence Needs Planning
Training Standards for Department of Defense Cyber Missions
TITLE X—GENERAL PROVISIONS
ITEMS OF SPECIAL INTEREST
OTHER MATTERS
Comptroller General Review of Medical Countermeasures Against Genetically Engineered Bio-Terror Agents
Comptroller General Review of Planning and Preparedness for Threats Posed by Non-Traditional Chemical Agents
Humanitarian Mine Action and Counter-Improvised Explosive Device Technologies
Sustainment of Sociocultural Understanding Capabilities
TITLE XII—MATTERS RELATING TO FOREIGN NATIONS
ITEMS OF SPECIAL INTEREST
Security Assistance and the Leahy Law
TITLE XVI—INDUSTRIAL BASE MATTERS
ITEMS OF SPECIAL INTEREST
Improving Information Technology Acquisition Outcomes
Space Surveillance Telescope

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE I—PROCUREMENT

OTHER PROCUREMENT, ARMY

Items of Special Interest

Civil Support Team information management needs

The committee is aware that the National Guard Bureau Weapons of Mass Destruction Civil Support Teams (WMD CST) currently field an information management system that provides a common operating picture, promotes information sharing and real-time collaboration in an emergency situation, and supports the CST mission of assisting and advising first responders and facilitating communications with other Federal resources. The committee has noted that it believes this system should be expanded to follow-on forces, such as the Chemical, Biological, Radiological, Nuclear, and High-Explosive Enhanced Response Force Package and Homeland Defense Response Force units. However, this has not yet occurred to date. Therefore, the committee directs the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs to provide a briefing to the Committee on Armed Services of the House of Representatives within 90 days

after the date of the enactment of this Act on the information management system needs of the Department of Defense WMD response forces, including the needs of both Active and Reserve Components.

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, ARMY

Items of Special Interest

Army directed energy testing

The committee is aware of the U.S. Army's current test effort through the Solid State Laser Testbed (SSLT) program, to examine the utility of directed energy technology as a supplement to current capabilities for force protection of rocket, artillery, and mortar threats. The committee stresses the importance of directed energy research and encourages the Army's continuation of those efforts. Therefore, the committee directs the Secretary of the Army to brief the Committees on Armed Services of the Senate and the House of Representatives within 90 days after the date of the enactment of this Act on SSLT program efforts. The briefing should include the following:

(1) Overview and results of the test campaign;

(2) The current status of plans to incorporate directed energy as a supplement to, or replacement for, the current counter-rocket, artillery, and mortar program of the Army;

(3) The projected mission utility based on current test results including the number of directed energy systems required to replace existing systems;

(4) Potential advantages and disadvantages in regards to magazine depth and associated costs; and

(5) Any logistical or operational challenges that remain to be addressed prior to deployment of a directed energy system, including satellite and aircraft interference as well as the maintenance of sophisticated laser technology in austere environments.

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, NAVY

Items of Special Interest

Maritime Laser Weapon System

The committee applauds the Navy's efforts in directed energy research and encourages the continuation of those efforts. The committee is also encouraged by the recent decision to deploy the Laser Weapon System (LaWS) for further testing and evaluation on the USS Ponce, in a stressing maritime environment. The committee believes such operational testing is necessary to work out the technical

challenges inherent in directed energy systems, in addition to identifying potential integration and policy challenges that might prove to be impediments to transitioning these types of systems to the fleet. Additionally, the committee recognizes that the Navy is developing other advanced technologies which will present similar integration challenges, in particular with regards to power generation, storage, and delivery. The committee encourages the Navy to begin developing a broadly applicable strategy for addressing these power challenges in order to facilitate technology integration onto naval vessels in the future. Furthermore, the committee directs the Secretary of the Navy to provide a briefing to the Committees on Armed Services of the Senate and the House of Representatives within 90 days after the date of the enactment of this Act on the testing efforts related to the LaWS deployment. The briefing should include:

(1) An overview of the test campaign plans and success criteria;

(2) Details of weapon system use and performance;

(3) A comparison of system performance with conventional weapons systems;

(4) A discussion of the associated power requirements with a comparison of the anticipated power requirements for other advanced weapons systems; and

(5) Unforeseen challenges associated with system maintenance and longevity in a maritime environment.

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

Items of Special Interest

Detection and threat identification technologies

The committee is aware that the Defense Threat Reduction Agency continues to have a strong partnership with each of the services as well as with U.S. Special Operations Command to develop and field technologies that reduce, counter and eliminate the threat of chemical, biological, radiological, nuclear and high-yield explosive materials (CBRNE). The committee remains concerned about credible threats posed by state and non-state actors in their attempts to acquire and weaponize CBRNE materials for use against the United States and its allies. Therefore, the committee encourages the Defense Threat Reduction Agency to continue the development, demonstration and deployment of innovative and emerging detection and threat identification technologies to ensure prompt transition of validated capabilities to address national security requirements.

The committee directs the Director, Defense Threat Reduction Agency to provide a briefing to the Committees on Armed Services of the Senate and the House of Representatives by December 31, 2013, on their efforts to advance and make operational a light-weight, person-portable CBRNE detection and analysis device.

Distributed Common Ground System enterprise

The committee is aware that the Distributed Common Ground System (DCGS) is a family of systems fielded across the military departments and other partners to provide an integrated architecture for all intelligence systems. DCGS is the current program of record for intelligence analytic, processing and dissemination capabilities for tactical and operational users. The committee is also aware that the "DCGS Enterprise," as the family of systems is known, has been under development and deployment for a number of years, and the cost, schedule and requirements continue to grow without keeping pace with the demands of the users or the current state of the art in technology.

To better understand those challenges, the committee requested the Comptroller General of the United States to review the DCGS Enterprise. The review found that "unlike a traditional weapon system acquisition, the DCGS Enterprise by its very nature has no clear end point and relies on a complex governance structure under a 'community of the willing' approach. This governance structure has had some success...however, not all of the services have kept pace in developing their systems and implementing improved interoperability standards that are available."

Therefore, the committee directs the Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the Under Secretary of Defense for Intelligence, to submit a report to the Committees on Armed Services of the Senate and the House of Representatives within 1-year after the date of the enactment of this Act on the information sharing framework and implementation plan for the DCGS Enterprise. The should report should include:

(1) The framework, including clearly defined criteria and metrics, to assess progress and outcomes pertaining to the level and quality of information sharing taking place across the DCGS Enterprise and its effect on intelligence operations;

(2) The applicability of this framework to non-DCGS Enterprise systems;

(3) An implementation plan that defines the way forward for getting to the desired end state for the DCGS Enterprise and articulates how the military services will be held accountable for doing their part in acquiring the systems necessary to achieve the end state. The plan should include the overall requirements, technologies, acquisition strategies, time frames, and investments needed by each of the military services to complete development and fielding of DCGS capabilities.

Foreign directed energy threats to U.S. military systems

The committee recognizes the importance of directed energy technology as a means to maintain an asymmetric operational and cost advantage over our adversaries. The committee, however, is aware that the United States is not the only nation which is pursuing this technology and is therefore concerned regarding the ability of the United States to maintain an advantage over potential adversaries should they employ similar technologies against U.S. forces.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the Committees on Armed Services of the Senate and the House of

Representatives within 180 days after the date of the enactment of this Act, on foreign directed energy threats and U.S. vulnerabilities to those threats. The briefing should consist of two sections. The first section should provide details regarding potential threats, current and projected, to U.S. military systems due to foreign directed energy weapons including high-energy lasers and high-power microwave systems. The Secretary of Defense should consult with the Director of National Intelligence regarding the information content of this section. The second section should discuss vulnerabilities of U.S. systems posed by foreign directed energy efforts, and the Department's initiatives to mitigate these vulnerabilities. The briefing should include a description of science and technology development efforts for directed energy countermeasures, as well a description of any technologies which are currently in use. The briefing should also address both tactical and strategic assets as well as efforts to protect U.S. personnel against directed energy attacks. The briefing should also identify any known technology gaps in directed energy countermeasures and any plans to address those gaps.

Standardization of directed energy weapon systems characterization

The committee is aware of several research, development, test, and evaluation (RDT&E) programs which pursue the development and eventual deployment of directed energy weapon systems. The committee understands the importance of the services and defense agencies ability to leverage RDT&E investments whenever possible to maximize the mutual benefit of these investments. Therefore, the committee encourages the services and defense agencies to continue to work synergistically in the development of these systems whenever possible. However, the committee is concerned about the inconsistency of definition of system performance amongst the different programs which make comparison of technologies and identification of leveraging opportunities between programs difficult. System descriptors such as "beam quality" for laser systems have multiple definitions within the directed energy community at large, and are not directly comparable between different systems. Some descriptors may only be applicable to a limited subset of missions and therefore inhibit the extrapolation of system performance to other missions. The ability to perform such comparisons is vital in the assessment of the different laser technologies applicability for missions of national interest.

Therefore, the committee directs the Secretary of Defense to develop a common set of parameters to describe directed energy weapon system performance with standardized definitions to be employed on all Department of Defense directed energy programs. The committee further directs the Secretary of Defense to submit a report to the Committees on Armed Services of the Senate and the House of Representatives within 12 months after the date of the enactment of this Act, which provides the rationale behind directed energy weapon system performance definitions.

OPERATIONAL TEST AND EVALUATION, DEFENSE

Items of Special Interest

Test and evaluation capabilities for electromagnetic pulse vulnerabilities

The committee is aware of that an electromagnetic pulse (EMP), both man-made and naturally occurring, as well as high-powered microwave (HPM) systems pose a significant challenge to the assurance of critical Department of Defense missions and assets. The committee recognizes that adequate test and evaluation facilities and capabilities are needed to maintain the standards for individual systems, as well as the networking of systems and infrastructure of the Department.

The committee is concerned that the Department has not adequately invested in the underlying infrastructure needed to support these test and evaluation capabilities, as well as the modeling and simulation tools required to support combatant commanders, wargames, military exercises and other assessments. Therefore, the committee directs the Director, Operational Test and Evaluation to provide a briefing to the Committee on Armed Services of the House of Representatives within 90 days after the date of the enactment of this Act, on the test and evaluation capabilities to support identification and mitigation of EMP and HPM vulnerabilities to the Department. The briefing should include identification of the existing capabilities and their sustainment levels, as well as identification of any gaps in those capabilities.

TITLE V—MILITARY PERSONNEL POLICY

ITEMS OF SPECIAL INTEREST

U.S. Special Operations Command Educational Initiatives

The committee supports U.S. Special Operations Command (USSOCOM) education initiatives that provide Special Operations Forces (SOF) with additional professional military education opportunities that serve to professionalize the force. While the committee supports these initiatives, it expects the educational opportunities to address requirements unique to SOF and that they will not duplicate educational opportunities provided by the military services unless the utilization tour required by the services for that educational opportunity proves burdensome for the SOF student. The committee is aware that USSOCOM is in the process of formalizing educational agreements with the Secretaries of the military departments to ensure effective coordination and to establish a process to formalize SOF education requirements.

The committee is pleased with this coordination, encourages a rapid coordination process, and looks forward to continued dialogue on the future of SOF education initiatives. Therefore, the committee directs the Chairman, Joint Chiefs of Staff, in coordination with the Commander, U.S. Special Operations Command,

to provide a briefing to the congressional defense committees within 90-days after the enactment of the enactment of this Act, outlining all SOF-unique educational requirements, recommendations for meeting those requirements, and how the proposed USSOCOM educational initiatives compare to service-offered educational opportunities.

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

ITEMS OF SPECIAL INTEREST

Advanced Technical Exploitation Program

The committee is aware the National Air and Space Intelligence Center (NASIC) is seeking to alter the acquisition strategy for the follow-on contract for the Advanced Technical Exploitation Program (ATEP). The committee is also aware that the objective of this follow-on contract, referred to as ATEP II, is "to provide contract services to support the NASIC mission in Geospatial Intelligence (GEOINT) and non-nuclear Measurement and Signature Intelligence (MASINT) Tasking, Collection, Processing, Exploitation, and Dissemination activities. This includes up to 24x7 intelligence operations, reach-back advanced data exploitation support, and cutting-edge GEOINT and MASINT research and development for NASIC and mission partners throughout the Department of Defense and intelligence communities."

The committee is also aware that the Air Force intends to use a lowest price, technically acceptable (LPTA) acquisition strategy for ATEP II and is planning to set this contract aside for small business concerns. The committee is concerned that the scope, scale, complexity and mission criticality of this work is inappropriate for an LPTA source selection and may not be well-suited for small business participation at the prime contract level. When those strategies are combined and used to procure complex, mission critical services, the risk of acquisition failure rises.

Therefore, the committee directs the Under Secretary of Defense for Acquisition, Technology, and Logistics to examine the Air Force's acquisition strategy related to provision of these services and to provide a briefing to the House Committee on Armed Services by October 1, 2013, that includes a detailed description of the following: (1) the acquisition strategy; (2) rationale and justification for using such strategy; (3) summary of market research methodology and findings performed during the development of the acquisition strategy; (4) assessment of risks related to such strategy; and (5) a description of the management and oversight structure necessary to ensure successful performance of the contracted activity throughout the period of performance.

Competition in Air Force Network-Centric Solutions Contracts

The committee is aware of reports that the Air Force may be inappropriately using sole source and brand name procurement solicitations and contract awards in the Network-Centric Solutions (NETCENTS), Air Force contract vehicles. The committee is concerned that these decisions may be negatively impacting competition between NETCENTS-1 and NETCENTS-2 contract vehicles. Therefore, the committee directs the Under Secretary of Defense for Acquisition, Technology and Logistics to review NETCENTS vehicles and provide a briefing to the Committee on Armed Services of the House of Representatives within 60 days after the date of the enactment of this Act. The review should detail the Air Force's use of "sole source" and "brand name only" procurement solicitations and contract awards under NETCENTS-1 and NETCENTS-2 contracts, as well as the extent to which the Air Force met the statutory requirements of Federal Acquisition Regulation (FAR) 6.303 and/or FAR 16.505, as applicable. The review should also detail remedial steps to be taken when the requirements of FAR 6.303 and/or FAR 16.505 have not been met, as applicable.

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

ITEMS OF SPECIAL INTEREST

Assessment of Cyber Centers of Academic Excellence

The committee is aware that the cyber security and information assurance manpower needs are growing increasingly in both total numbers as well as in disciplines where new skills are needed.

In order to develop an adequate pool of appropriately skilled individuals, the National Security Agency and the Department of Homeland Security have jointly established a program to certify institutions of higher learning that provides curricula for information assurance education. The certification program for Centers of Academic Excellence (CAE) includes a rigorous application and screening process, which focuses on identifying schools offering a highly technical and interdisciplinary curriculum. The committee believes that leveraging CAEs may help the Department of Defense achieve its near-term goals of increasing the number of qualified cyber personnel. However, the committee believes that the current certification program should be assessed to determine its strengths as well as areas where improvement is needed.

Therefore, the committee directs that the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer, in consultation with the Secretaries of the military services and the Director, National Security Agency, to provide an assessment to the congressional defense committees within 180 days after the date of the enactment of this Act, on the National Security Agency/Department of Homeland Security Centers of Academic Excellence program. The report should include an assessment of criteria for certification of institutions,

mechanisms for increasing collaboration between Department of Defense and certified institutions, and mechanisms for increasing the number of graduates from CAE-certified institutions into the the Department of Defense's cyber workforce.

Coordination of Cyber and Electronic Warfare Capabilities

The committee notes that significant advances have been made in both the cyber and electronic warfare (EW) domains. The committee is aware that there is increasing overlap between these domains, particularly with the advanced capabilities of next-generation EW platforms. Therefore, the committee directs the Secretary of Defense to provide a briefing to the congressional defense committees within 90 days after the date of the enactment of this Act, on the status and level of coordination of research, development, test and evaluation efforts within the EW and cyber disciplines that bridge, or have corresponding dependencies, across these fields.

Cyber Standards Framework

The committee is aware of the recent Executive Order "Improving Critical Infrastructure Cybersecurity," included language that directs the development of a framework for reducing cyber risks to critical infrastructure within the next year. The committee expects that the Cybersecurity Framework, developed under the leadership of the Director of the National Institute of Standards and Technology, will incorporate a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks, including, where possible, voluntary consensus standards and industry best practices. The committee encourages the Secretary of Defense to explore ways in which to incentivize, wherever possible, the adoption of the Cybersecurity Framework, such as through contracts and other agreements with relevant outside vendors and utilities. Furthermore, the committee directs the Secretary of Defense to provide a briefing to the congressional defense committees within 180 days after the date of the enactment of this Act on actions being considered to encourage adoption of the Cybersecurity Framework.

Defense Intelligence Collection Management

The committee recognizes the importance of effective collection management in the Department of Defense to enable optimal collection against intelligence targets that are a priority of the military services and combatant commands. The committee is aware that the Department identifies a collection management strategy as the method used by a collection manager to establish, prioritize, and submit collection requirements in a deliberate, focused, integrated, and synchronized manner across multiple intelligence disciplines. The goals of this strategy are: (1) to identify, allocate, and apply national, theater and tactical intelligence, surveillance, and reconnaissance resources and capabilities; (2) to task

these resources, submit requirements, and collect in a way that effectively and efficiently answers the priority intelligence requirements; (3) to support analytic intelligence information shortfalls and gaps; and (4) to support the development of effective and responsive collection plans to ground the adaptive planning process.

Based on feedback from the combatant commands, the committee is concerned that the Department has not established the proper tools and training to fully enable the most effective collection and mission management. Therefore, the committee directs the Under Secretary of Defense for Intelligence to provide a briefing to the congressional defense and the congressional intelligence committees by February 1, 2014, on the Department's activities to support effective intelligence collection management and mission management.

Input into National Intelligence Priorities Framework

The committee continues to support and commend efforts of the Department of Defense and the intelligence community to further integrate and coordinate intelligence activities. The committee believes that as integration continues, it is essential to periodically assess and ensure that the Department of Defense and the intelligence community are meeting the intelligence needs of the warfighter.

Therefore, the committee directs the Chairman, Joints Chiefs of Staff to submit an assessment to the congressional defense committees and the congressional intelligence committees by October 1, 2013, evaluating the extent to which the coordination process for the National Intelligence Priorities Framework (NIPF) incorporates the intelligence priorities of the Joint Staff, the combatant commands, and the military departments. Such assessment should include a description of the input from the Joint Staff, the combatant commands, and the military departments regarding significant intelligence priorities; the process used to communicate such input; and the results of such input. The assessment should also include specific feedback from each of the combatant commands and military departments regarding the NIPF coordination process and any recommendations for improving the input of the Joint Staff, combatant commands, and military departments to that process.

Integrated Science and Technology Campus for the Defense Intelligence Agency

The committee recognizes the important role that science and technology research play in advancing the mission of the Defense Intelligence Agency (DIA). As threats become increasingly more complex and sophisticated, DIA science and technology programs will need to work in synergy and leverage assets available in the interagency, academic, and industrial research community to address new interdisciplinary challenges.

The committee believes that the Base Closure and Realignment (BRAC) 2005 vision of an integrated science and technology campus for DIA is critical component of its ability to provide indications and warning of future technology

threats, as well as in-depth analyses that could monitor and develop countermeasures or mitigation measures for those threat technologies, as necessary.

Therefore, the committee directs the Under Secretary of Defense for Intelligence to brief the Committees on Armed Services of the Senate and the House of Representatives within 120 days after the date of the enactment of this Act, on the progress of the BRAC 2005 vision. The briefing should address the following:

(1) How DIA is leveraging other Government agency expertise to fulfill its mission;

(2) How DIA is utilizing or plans to utilize, academic, industry, and non-profit research organization capabilities to enhance its science and technology focus;

(3) To what extent DIA is at space capacity at its current facilities;

(4) What facilities have been considered, designed, or constructed to realize the integrated campus; and

(5) What resources are required to achieve the BRAC 2005 vision.

Open-Source Intelligence Utilization

The committee notes that open-source intelligence (OSINT) is intelligence that is produced from publicly available information collected, exploited, and disseminated to an appropriate audience for the purpose of addressing a specific intelligence requirement. The National Defense Authorization Act for Fiscal Year 2006 (Public Law 109-163) directed the Secretary of Defense to develop a strategy for OSINT to be incorporated into the larger military intelligence strategy. The committee recognizes that the accessibility of open-source information has increased significantly in recent years due to rapid growth of international internet use and consideration as a global commons. Therefore, the committee directs the Under Secretary of Defense for Intelligence to provide a briefing to the congressional defense and the congressional intelligence committees within 180 days after the date of the enactment of this Act, on the current status of the OSINT strategy and operations within the Department of Defense. The briefing should include the following:

(1) An overview of the current strategy for OSINT collection, to meet the intelligence priorities of the military services and combatant commands;

(2) A description of all OSINT activities within the military services and combatant commands including the level of coordination and deconfliction between ongoing joint efforts;

(3) A description of the current level of coordination with the Director of National Intelligence Open Source Center;

(4) Gaps in OSINT capabilities within the Department;

(5) Research, development, test and evaluation efforts in the Department related to collection, processing and sharing of open-source intelligence; and

(6) Recommendations for future improvements in the Department's OSINT strategy and efforts.

Pilot to Counter Brokers of Transnational Criminal Organizations

The committee is aware that the complex pathways and instrumentalities of the global economic system provide both a source of revenue and backdrop in which to hide for a number of nation-state and non-state actors. In particular, Transnational Criminal Organizations (TCOs) have increasingly been able to use the global economic environment to their advantage. TCOs have grown more complex over time, and so has our ability to defeat them, however, this complexity has challenged our ability to access and use collective information available.

The committee believes that criminal cartel organizations are hosting themselves in U.S. cities and may be teaming with terrorists also embedded in the United States to fund terror networks overseas. These networks provide sustained and substantial funding to pay operatives, support families, purchase and traffic weapons, indoctrinate and recruit new members, train, travel, and bribe officials and also perpetrate billions of dollars worth of fraud against banks, businesses and Governments. The list of crimes that the new international criminal organizations are involved in includes the trafficking of narcotics, humans, weapons, illegally poached animal remains, and chemical, biological, and nuclear material. Disrupting the means and mechanisms through which these networks move money will significantly disrupt their operations, but remains the most challenging piece of the puzzle to unravel.

The key to dissecting these financial networks is to identify the "brokers;" a category of individuals who facilitates financial activities. Brokers may be employees of a single TCO, such as a terrorist group or drug cartel, or they may be independent operators charging variable fees based on external factors such as interest rates, dollar amount, and denomination of currency. These individuals may work in banking, real estate, insurance, own small businesses, or simply have legitimate access to the financial system. The information needed to unravel these global networks is available through various technical, commercial, open source and Government-owned means, yet require experienced subject matter experts to "connect the dots;" an ability directly proportional to their access to information across the community of interest.

Therefore, the committee directs the Under Secretary of Defense for Intelligence, in coordination with the Under Secretary of Defense for Policy, to establish a pilot program to determine the information requirements for identifying and countering TCO brokers, and to submit a report to the Committees on Armed Services of the Senate and the House of Representatives within 1 year after the date of the enactment of this Act on the results of the pilot program.

Science and Technology Community Intelligence Needs Planning

The committee applauds recent efforts by the Department of Defense science and technology (S&T) community to reinvigorate its relationship with the intelligence community. The committee is aware that in 2010, the Assistant Secretary of Defense for Research and Engineering drafted an Intelligence Needs

Plan in order to formally convey the S&T communities' intelligence requirements to the intelligence community. The committee believes that such efforts are important in order to position science and technology for the development of capabilities for new and emerging threat areas. The committee is concerned that the focus of intelligence activities for the past 10 years has been primarily focused on near-term, operationally-oriented support that consequently, the capabilities to do long-term, open-ended estimations have atrophied. Creating a demand signal for such analyses would both rebuild needed intelligence skills and support better S&T planning.

Therefore, the committee directs the Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the Under Secretary of Defense for Intelligence, to provide a briefing to the Committees on Armed Services of the Senate and the House of Representatives, the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate by February 1, 2014, on the intelligence requirements of the science and technology community, as well as the process by which the intelligence community would satisfy those requirements.

Training Standards for Department of Defense Cyber Missions

The committee notes that the Department of Defense is in the process of staffing a number of national cyber forces under U.S. Cyber Command, including national mission teams, combatant command mission teams, and cyber protection platoons. The committee is also aware that as part of this process , the Department is working to establish a joint standard to provide some level of standardization and compatibility among forces being supplied by the military services. The committee encourages the Department to continue developing these training standards for cyber forces, but believes that the Department should consider the scalability and sustainability of such training. The committee is aware that the Department already faces serious challenges in building and sustaining its cyber forces, and the increased demands from U.S. Cyber Command make that challenge even more acute. Furthermore, the committee recognizes that the military services already have training demands to meet their own statutory requirements to man, train and equip forces for their networks, and that those requirements must be taken into consideration as well.

The committee is concerned that the process for determining a joint training standard may be settling on a proposed standard too quickly, without sufficient analysis to support the scalability demands on the services. In addition, the committee believes that such a standard should include an assessment of the current training and education capabilities inherent in the services to determine if the current infrastructure meets the personnel training pipeline, as well as if there are any gaps that will need to be resourced in the future. The committee also notes that any standard should include the means for leveraging commercial standards and certifications to reduce the burden on departmental infrastructure.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the congressional defense committees within 180 days after the date of the enactment of this Act, on the cyber force training needs of the Department. The briefing should include the current and proposed training standard and the Department's process for expanding the training across the force. The committee also expects that future quarterly cyber operations briefings will include updates on the manning and training metrics for U.S. Cyber Command national mission teams.

TITLE X—GENERAL PROVISIONS

ITEMS OF SPECIAL INTEREST

OTHER MATTERS

Comptroller General Review of Medical Countermeasures Against Genetically Engineered Bio-Terror Agents

The committee recognizes that development and deployment of safe, effective medical countermeasures against biological weapons and agents of concern remain an urgent priority for the U.S. Government. The National Institutes of Health (NIH), under the direction of the Department of Health and Human Services, is working with the Department of Homeland Security and the Department of Defense (DOD), as well as other agencies, to shape and execute an aggressive research program to develop more effective medical countermeasures.

The committee notes that since 2007, the Department of Defense has initiated efforts to strengthen homeland defense and homeland security by developing broad-spectrum medical countermeasures against the threat of genetically engineered bio-terror agents. Additional initiatives that the Department of Defense is planning include the development of advanced detection and deterrent technologies and initiatives to facilitate full-scale civil-military exercises. While the Department of Defense planned to spend over $1.0 billion on these initiatives between fiscal years 2007-12, it remains unclear how it has coordinated its programs to complement those of the National Institutes of Health and the Department of Health and Human Services. The degree to which the Department of Defense has met program goals to improve interagency planning for complex homeland security contingencies also remains unclear.

The committee remains committed to a robust medical research and development program focused on military health issues, including medical biological, and chemical defense. However, to assist the committee in conducting its oversight of DOD's initiatives to develop medical countermeasures, coordinate programs, and improve interagency contingency planning, the committee directs the Comptroller General of the United States to conduct a comprehensive review of medical countermeasures against genetically engineered bio-terror agents, and to

submit a report to the congressional defense committees by March 3, 2014, on the findings and any recommendations. The report should include, but not be limited to:

(1) The status of DOD's initiatives to develop countermeasures for genetically engineered bio-terror agents and advanced detection and deterrent technologies;

(2) The extent to which the National Institutes of Health and the Department of Defense have coordinated their research programs to ensure efforts are complementary and not duplicative;

(3) The extent to which the Department of Defense, the National Institutes of Health, the Department of Homeland Security and other agencies have planned and executed full-scale civil-military exercises to improve interagency coordination;

(4) The cost basis for DOD's various programs and initiatives to develop countermeasures for genetically engineered bio-terror agents and related detection and deterrent technologies; and

(5) The nature and extent of potential program overlap and duplication with programs of other Federal agencies that could benefit from consolidations or improved coordination to achieve cost savings.

Comptroller General Review of Planning and Preparedness for Threats Posed by Non-Traditional Chemical Agents

The committee notes a growing awareness of the threat posed by novel chemical weapon agents or toxicants known as Non-Traditional Agents (NTAs) or Fourth Generation Agents. The 2010 Quadrennial Defense Review (QDR) states that the globalization of the world's chemical industry, coupled with scientific breakthroughs, increases the possibility of NTAs being used against U.S. and allied forces. Furthermore, the QDR states that the Department of Defense (DOD) has increased its resources for research and development of technologies to meet and defeat these emerging threats. NTAs are allegedly binary nerve agents significantly more lethal than third-generation chemical weapons, such as VX nerve gas.

The current international agreements regarding chemical warfare do not adequately control for the relatively simple formulas for NTAs that have been published. Consequently, the risk of illicit NTA production by various state and non-state actors is heightened compared to traditional chemical agents. NTAs could pose a significant threat to DOD personnel as they may be capable of defeating protective equipment, such as Mission Oriented Protective Posture masks and suits as well as evading chemical weapon detection tools. In the past, the Government Accountability Office has reported that most U.S. Army units tasked with providing chemical and biological defense support are not adequately staffed, equipped, or trained to perform their missions against traditional chemical agents. The Deparment's preparedness for NTAs may be even more important given the unique nature of this emerging threat.

To assist the committee in conducting its oversight of the Department of Defense's increased resources for research and development of technologies to meet

and defeat emerging threats posed by NTAs, novel chemical weapon agents, or similar toxicants, the committee directs the Comptroller General of the United States to conduct a review of the Department of Defense's planning and preparedness for threats posed by non-traditional chemical agents, and to submit a report to the congressional defense committees by March 31, 2014, with the findings and any recommendations. The report should include, but not be limited to:

(1) The extent to which the Department of Defense has conducted an analysis of the threat NTAs pose to DOD personnel, including the risk posed by bioregulators capable of inducing profound physiologic effects, and developed countermeasures, defenses, and mitigation strategies to address the threat posed by NTAs;

(2) The extent to which DOD's chemical and biological defense units that are tasked with chemical and biological defense support to combat units and commands are adequately staffed, equipped, and trained to deal with NTAs;

(3) The extent to which DOD's chemical and biological defense units that are tasked with a homeland defense mission, especially National Guard and Reserve units, are adequately staffed, equipped, and trained to deal with NTAs;

(4) How much the Department is planning to spend in fiscal year 2014 on research and development of technologies to address the threat of NTAs, and how much of an increase in resources this represent over fiscal year 2013 levels;

(5) The nature and extent of potential counter-NTA research and development program overlap and duplication between, for example, defense agencies, the military services, and national laboratories/federally funded research and development centers; and

(6) Which counter-NTA programs or efforts could benefit from consolidations, improved coordination, or other actions to achieve financial or other benefits, such as increased efficiencies.

Humanitarian Mine Action and Counter-Improvised Explosive Device Technologies

The committee remains concerned that the Department of Defense Humanitarian Mine Action (HMA) program is under-utilized and under-resourced, to include research, development, testing, and evaluation efforts. The committee notes that while the committee has authorized $10.0 million per fiscal year for this program in the past, the Department of Defense routinely commits less than $3.0 million per year towards global HMA requirements. Because of these shortfalls, the committee notes that HMA programs and projects are unable or unlikely to contribute to Geographic Combatant Commander theater security cooperation strategies in a substantive and enduring way, and that the efforts of Department of Defense are potentially out of balance with larger U.S. Government HMA and security force assistance goals. Furthermore, the Department of Defense and commercial industry have invested heavily in improvised explosive device defeating technology over the past decade, and the committee believes that this technology should be better utilized within the HMA program.

Therefore, the committee directs the Secretary of Defense, in coordination with the Secretary of State, to submit a report to the congressional defense committees within 90 days after the date of the enactment of this Act, that outlines the strategic direction of the Department of Defense's HMA program, to include efforts to improve research, development, test, and evaluation, and ways to ensure coordination mechanisms exist to determine whether counter-improvised explosive technology could be applicable to HMA. In addition, the report should outline ways to improve interagency coordination with similar programs underway in the Department of State and the U.S. Agency for International Development.

Sustainment of Sociocultural Understanding Capabilities

The committee is aware that the Department of Defense has invested in a number of programs over the past 10-years to provide increased sociocultural understanding at tactical, operational and strategic levels. The committee has been supportive of many of these capabilities, such as the Army's Human Terrain System, the Secretary of Defense's Minerva Initiative, and the cross-service Human, Social, Cultural, Behavioral Modeling program. Each program has served an important role in filling capability gaps for the Department, especially with regards to understanding the human dimensions of the counterinsurgency fights in the Republic of Iraq and the Islamic Republic of Afghanistan.

However, the committee is concerned that with the drawdown of forces in Afghanistan and the refocus to the Asia-Pacific region, there may be a growing sense that some of the capabilities that proved so useful in the Middle East will be of little or no value in potential contingencies rooted in the Asia Pacific region. The committee firmly believes that sociocultural understanding will remain important in the Middle East as it grows in importance in Africa and Asia, though needs will be somewhat different and may require slightly different instantiations based on the differences in the operational environment.

Therefore, the committee directs the Secretary of Defense to submit a report to the congressional defense committees within 180 days after the date of the enactment of this Act, on the Department's plans for maintaining and adapting existing sociocultural capabilities, as well as development for new capabilities to meet the current strategic guidance. The report should identify the programs either in development or that have been deployed that support sociocultural understanding, and whether they will be sustained across the Future Years Defense Program. Elements of the report should also identify any capability gaps that exist based on the recent guidance shifting the Department's focus to the Asia-Pacific region.

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

ITEMS OF SPECIAL INTEREST

Security Assistance and the Leahy Law

The committee supports the intent of the Limitation on Assistance to Security Forces as set forth in section 2378d of title 22, United States Code, and section 8058 of the Consolidated Appropriation Act, 2012 (Public Law 112-74) collectively and commonly known as the "Leahy Law." The committee notes that the Leahy Law, through its prohibition on security assistance to foreign forces that have been implicated in gross violations of human rights, promotes respect for human rights abroad. Further, the committee believes that the law can assist in professionalizing foreign military and security forces by linking the resumption of security assistance to action to correct human rights abuses.

The committee notes that the Department of State conducts the human rights vetting process on behalf of the Department of Defense. In keeping with these laws, current policies require the vetting of unit commanders and their units when full-unit training is requested, and the vetting of individual security force members and their respective units when individual training is requested.

While the committee supports the intent of the law and the coordination processes between the Department of Defense and the Department of State, the committee is concerned about the implementation of the law. Two recent committee hearings have highlighted a potential divergence between the intent of the law and its application to certain Department of Defense security assistance activities planned with full Chief of Mission concurrence. At those hearings, geographic combatant commanders testified before the committee and the Subcommittee on Intelligence, Emerging Threats and Capabilities that the law, "is at times stopping us perhaps more broadly than was the congressional intent," and that the law, "has restricted us in a number of countries across the globe in our ability to train units that we think need to be trained, that the U.S. Ambassador in many cases thinks needs to be trained, that those nations think need to be trained, and yet because of some of the restrictions of the Leahy amendment, we are prohibited from doing that."

The committee additionally notes a difference in language between section 2378d of title 22, United States Code, and section 8058 of Public Law 112-74 that may create a potential for misinterpretation. While section 2378d of title 22 notes that a prohibition shall remain in effect until "the Government of such country is taking effective steps to bring the responsible members of the security forces unit to justice," the concomitant section 8058 of Public Law 112-74 makes no funds available, "unless all necessary corrective steps have been taken." The committee believes that amended and clarifying language may be required to address any potential divergence between the intent of the law and its application.

The committee expects to remain engaged on this issue and to work with the Departments of Defense and State, the relevant congressional defense committees, and the Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate to ensure that Department of

Defense needs and requirements are fully addressed, while continually complying with the intent of the Leahy Law.

Therefore, the committee directs the Secretary of Defense, in coordination with the Secretary of State, to provide a briefing to the congressional defense committees within 90 days after the date of the enactment of this Act, on the implementation of the Leahy Law with respect to Department of Defense security assistance programs. The briefing should outline current implementation policies, limitations and recommendations for improvements.

TITLE XVI—INDUSTRIAL BASE MATTERS

ITEMS OF SPECIAL INTEREST

Improving Information Technology Acquisition Outcomes

The committee is aware that the Department of Defense continues to face challenges in its efforts to effectively acquire information technology (IT) resources. Even as the importance of such IT systems increases, from providing mission critical systems for intelligence analysis and fusion to time and cost-savings capabilities for electronic health records and financial auditability, the Department's success rate in developing, acquiring and implementing these systems remains mediocre, at best. This point is underscored by the failure of recent IT initiatives by the Department, such as the Expeditionary Combat Support System, the Defense Integrated Military Human Resources System, or the Net-Enabled Command Capability.

The committee believes that part of the challenge that the Department faces is in its reliance on processes that are to heavily focused on the acquisition of militarily-unique hardware systems. The committee recognizes that the paradigm for IT acquisition is rooted more firmly in the commercial marketplace. As a consumer of commercially-developed solutions, rather than a generator of unique requirements, the Department follows commercial trends more often than it leads them.

Unfortunately, the committee believes that the Department has not done enough to come to terms with this trend, choosing instead to act as though it has the same power to influence computing and electronics markets as it did for most of the 20th century. Though numerous studies have indicated a need to change acquisition processes within the Department to adjust to the reality of 21st century commercial IT markets, the Department has made little progress. Section 804 of the National Defense Authorization Act of Fiscal Year 2012 (Public Law 111-84) authorized the Department to implement a new acquisition process for IT systems, but to date, there has been little tangible action to take advantage of those new authorities.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the Committees on Armed Services of the Senate and the House of

Representatives within 90 days after the date of the enactment of this Act, on the progress of implementing an IT-specific acquisition process, as well as how lessons are being learned from recent IT failures in order to improve the outcomes for current and future efforts.

Space Surveillance Telescope

The committee is aware that the Defense Advanced Research Projects Agency (DARPA) has developed a Space Surveillance Telescope (SST) program in order to demonstrate an advanced ground-based optical system to detect and track faint objects in space. The committee understands that DARPA has signed a memorandum of agreement with the Air Force to transition SST to Air Force Space Command for operational use. Furthermore, the committee understands that SST will be moved to the Commonwealth of Australia for further operational demonstrations in a relevant environment with a richer and more interesting population of SSA targets in geosynchronous orbit.

However, the committee believes this move presents numerous challenges, including logistical and technical communications obstacles resulting from a site that is significantly more remote than the current SST location. Therefore, the committee directs the Secretary of Defense, in coordination with the Secretary of the Air Force, to provide a briefing to the Committees on Armed Services of the Senate and the House of Representatives within 120 days after the date of the enactment of this Act, on the logistical and sustainment strategy for SST. The briefing should address the plans for providing the maintenance and spare parts for SST after it is moved to Australia.