H.R. 1540—FY12 NATIONAL DEFENSE AUTHORIZATION BILL

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Title I	Procurement
Title II	Research, Development, Test, and Evaluation
Title III	Operation and Maintenance
Title VII	Health Care Provisions
Title VIII	Acquisition Policy, Acquisition Management, and Related Matters
Title IX	Department of Defense Organization and Management
Title X	General Provisions
Title XII	Matters Relating to Other Nations
Title XIV	Other Authorizations

Summary of Bill Language	p. 3
Bill Language	p. 9
Summary of Directive Report Language	p. 55
Directive Report Language	p. 57

SUMMARY OF BILL LANGUAGE

Titles 1, 2, 3, 8, 9, 10, 12 & 14

TITLE I—PROCUREMENT

Section 144—Limitation on Availability of Funds for Aviation Foreign Internal Defense Program

This section would require a report outlining U.S. Special Operations Non-Standard Aviation and Aviation Foreign Internal Defense programs and strategies. This section would also prohibit U.S. Special Operations Command from obligating more than 50 percent of the funds available for fiscal year 2012 for procurement of fixed wing non-standard aviation platforms until the required report has been submitted to the congressional defense committees.

Section 145—Limitation on Availability of Funds for Commercial Satellite Procurement

This section would prohibit the Defense Information Systems Agency from obligating more than 20 percent of the funds available for fiscal year 2012 for commercial satellite procurement until the Secretary of Defense provides an independent assessment of the acquisition strategy.

Section 146—Separate Procurement Line Item for Non-Lethal Weapons Funding

This section would direct the Secretary of Defense to provide a dedicated procurement line item in future defense budget submissions for non-lethal weapons (NLW). The committee expects that each line item description will identify the specific programs for which funds are being requested; provide summary justification for the program; identify whether the program is a joint or service-specific initiative; and the amount of funding provided during the past fiscal year. The committee also expects the Department to provide similar information for all budget requests for research, development, test and evaluation for NLWs.

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

Section 217—Limitation on Availability of Funds for Wireless Innovation Fund

This section would prohibit the Defense Advanced Research Projects Agency from obligating more than 10 percent of the funds available for fiscal year 2012 for the Wireless Innovation Fund until the Under Secretary of Defense for Acquisition, Technology, and Logistics provides a report on how the fund will be managed and executed.

Section 221—Prohibition on Delegation of Budgeting Authority for Certain Research and Education Programs

This section would prohibit the Secretary of Defense from delegating the authority for programming or budgeting of the Historically Black Colleges and Universities and Minority Serving Institutions program to an individual outside the Office of the Secretary of Defense.

Section 242—Independent Review and Assessment of Cryptographic Modernization Program

This section would require the Secretary of Defense to conduct an independent assessment of the cryptographic modernization program for the Department of Defense and submit a report to Congress by March 1, 2012.

Section 251—Repeal of Requirement for Technology Transition Initiative

This section would repeal section 2359a of title 10, United States Code upon delivery of the report required by section 253 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110-417). The committee notes with consternation that this report required by law is nearly 2 years overdue.

TITLE III—OPERATION AND MAINTENANCE

Section 343—Limitation on Obligation and Expenditure of Funds for Migration of Army Enterprise Email Services

This section would prohibit the Army from obligating more than 2 percent of the funds available for fiscal year 2012 in procurement and operations and maintenance accounts for the migration of enterprise email services until the Secretary of the Army provides a business case analysis comparing the relative merits and cost-benefit analysis of transitioning to Defense Information Systems Agency enterprise email services.

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

Section 811—Calculation of Time Period Relating to Report on Critical Changes for Major Automated Information Systems

This section would amend the requirement for when a critical change report would be needed for a Major Automated Information System (MAIS). Currently, a report is required when a MAIS investment has failed to achieve a full deployment decision within 5 years after funds were first obligated for the program. This section would amend that to require a critical change report within 5 years after contract award. This section would also specify that any time under which the contract award is under protest would not be counted against this 5-year limit.

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

Section 901—Revision of Defense Business System Requirements

This section would update the structure and process of the defense business systems investment review boards, including clarifying responsibilities based on recent reorganization within the Department of Defense. This section would also consolidate reporting by the Department of Defense Deputy chief management officers and the reports required by the Chief Management Officer of the military departments required by section 908 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110-417).

Section 963—Activities to Improve Multilateral, Bilateral, and Regional Cooperation regarding Cybersecurity

This section would establish a cybersecurity fellowship program within the Department of Defense that would allow for the temporary assignment of a member of the military forces of a foreign country to a Department of Defense organization for the purpose of assisting the member to obtain education and training to improve the member's ability to understand and respond to information security threats, vulnerabilities of information security systems, and the consequences of information security incidents.

Section 964—Report on United States Special Operations Command Structure

This section would require the Secretary of Defense provide to the congressional defense committees by March 1, 2012, a report on U.S. Special Operations Command structure and make recommendations to better support development and deployment of joint special operations forces.

TITLE X—GENERAL PROVISIONS

Section 1032—Extension of Authority for Making Rewards for Combating Terrorism

This section would extend the authority for the Secretary of Defense to offer and make rewards to a person providing information or nonlethal assistance to U.S. Government personnel or Government personnel of Allied Forces participating in a combined operation with U.S. armed forces through fiscal year 2014 and change the annual reporting timeline from December to February.

Section 1041—Counterterrorism Operational Briefing Requirement

This section would require the Secretary of Defense to provide quarterly briefings to the congressional defense committees quarterly briefs outlining Department of Defense counterterrorism operations and related activities involving Special Operations Forces not later than March 1, 2012.

Section 1077—Assessment of the Defense Industrial Base Pilot Program

This section would require the Secretary of Defense to submit a report to the congressional defense committees assessing the defense industrial base pilot program of the Department of Defense by March 1, 2012.

Section 1092—Treatment under Freedom of Information Act of Certain Department of Defense Critical Infrastructure Information

This section would exempt certain Department of Defense critical infrastructure information from disclosure pursuant to Section 552(b)(3) of title 5, United States Code.

Section 1093—Expansion of scope of humanitarian demining assistance program to include stockpiled conventional munitions assistance

This section would update the Department of Defense definition of "Humanitarian Demining Assistance" to include physical security, stockpile management and explosive safety as components of assistance and training.

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

Section 1201—Expansion of Authority for Support of Special Operations to Combat Terrorism

This section would increase the amount authorized for support of special operations to combat terrorism pursuant to section 1208 of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (Public Law 108-375; 118 Stat. 2086), as most recently amended by section 1201 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111-383; 124 Stat. 4385), from $45 million to $50 million, extend the authority through fiscal year 2014, and direct the Department of Defense to provide an implementation strategy that outlines the future requirements that would require similar authority in preparation for pending authority expiration.

Section 1204—Five-Year Extension of Authorization for Non-Conventional Assisted Recovery Capabilities

This section would authorize the Department of Defense 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 United States national interests globally. The initial authorization contained in section 943 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110-417) provided for funds for this program to be available through fiscal year 2011. This section would allow the Secretary of Defense to use funds through fiscal year 2016.

TITLE XIV—OTHER AUTHORIZATIONS

Section 1404—Chemical Agents and Munitions Destruction, Defense

This section would authorize appropriations for Chemical Agents and Munitions Destruction, Defense at the level identified in section 4501 of division D of this Act.

Section 1421—Changes to Management Organization to the Assembled Chemical Weapons Alternative Program

This section would allow the Assembled Chemical Weapons Alternative Program (ACWA) to work closely with the U.S. Army Chemical Materials Agency (CMA). The Committee believes that CMAs leadership, engineers, scientists, project managers, technical managers, and safety technicians represent a pool of talent and experience that can and should be leveraged as CMA begins to draw down upon the completion of its mission to help address and anticipate risks and help to underwrite future success of ACWA.

BILL LANGUAGE

Titles 1, 2, 3, 8, 9, 10, 12 & 14

1 **SEC. 144 . LIMITATION ON AVAILABILITY OF FUNDS FOR**
2 **AVIATION FOREIGN INTERNAL DEFENSE**
3 **PROGRAM.**

4 (a) LIMITATION.—Of the funds authorized to be ap-
5 propriated by this Act or otherwise made available for fis-
6 cal year 2012 for the procurement of fixed-wing non-
7 standard aviation aircraft in support of the aviation for-
8 eign internal defense program, not more than 50 percent
9 may be obligated or expended until the date that is 30
10 days after the date on which the Commander of the United
11 States Special Operations Command submits the report
12 under subsection (b)(1).

13 (b) REPORT REQUIRED.—

14 (1) REPORT.—Not later than January 15,
15 2012, the Commander of the United States Special
16 Operations Command shall submit to the congres-
17 sional defense committees a report on the aviation
18 foreign internal defense program.

19 (2) MATTERS INCLUDED.—The report under
20 paragraph (1) shall include the following:

21 (A) The results of an analysis of alter-
22 natives and efficiencies review conducted prior
23 to fiscal year 2012 with respect to a contract

1 awarded for the aviation foreign internal de-
2 fense program.
3 (B) An explanation of plans or business-
4 case analyses justifying new procurements rath-
5 er than leased platforms, including an expla-
6 nation of any efficiencies and savings.
7 (C) A comprehensive strategy outlining
8 and justifying the overall projected growth of
9 the aviation foreign internal defense program to
10 satisfy the increased requirements of the com-
11 manders of the geographic combatant com-
12 mands.
13 (D) An examination of efficiencies that
14 could be gained by procuring platforms such as
15 those being procured for light mobility aircraft.
16 (3) FORM.—The report under paragraph (1)
17 shall be submitted in unclassified form, but may in-
18 clude a classified annex.

1 **SEC. 145 . LIMITATION ON AVAILABILITY OF FUNDS FOR**
2 **COMMERCIAL SATELLITE PROCUREMENT.**

3 Of the funds authorized to be appropriated by this
4 Act or otherwise made available for fiscal year 2012 for
5 the procurement of a commercial satellite by the Director
6 of the Defense Information Systems Agency or the Sec-
7 retary of the Air Force, not more than 20 percent may
8 be obligated or expended until the date that is 30 days
9 after the date on which the Secretary of Defense submits
10 to the congressional defense committees an independent
11 assessment of the analysis of alternatives for the procure-
12 ment of such satellite, including—

13 (1) an assessment of why noncommercial sat-
14 ellites owned and operated by the Federal Govern-
15 ment would not meet the needs of the Department
16 of Defense;

17 (2) a concept of operations for all alternatives
18 considered;

19 (3) a cost-benefit comparison of such alter-
20 natives;

21 (4) an analysis comparing the risks and
22 vulnerabilities of such alternatives, including risks
23 and vulnerabilities related to security, operation in

1 denied environments, and continuity of operations
2 capability;
3 (5) mitigation measures, including estimated
4 cost impacts, for such risks and vulnerabilities com-
5 pared under paragraph (4); and
6 (6) any other matters the Secretary considers
7 appropriate.

1 **SEC. 146 . SEPARATE PROCUREMENT LINE ITEM FOR NON-**
2 **LETHAL WEAPONS FUNDING.**

3 In the budget materials submitted to the President
4 by the Secretary of Defense in connection with the submis-
5 sion to Congress, pursuant to section 1105 of title 31,
6 United States Code, of the budget for fiscal year 2013,
7 and each subsequent fiscal year, the Secretary shall ensure
8 that within each military department procurement ac-
9 count, a separate, dedicated procurement line item is des-
10 ignated for non-lethal weapons.

1 **SEC. 2 17 . [Log #237] LIMITATION ON AVAILABILITY OF**
2 **FUNDS FOR WIRELESS INNOVATION FUND.**

3 Of the funds authorized to be appropriated by this
4 Act or otherwise made available for fiscal year 2012 for
5 the wireless innovation fund within the Defense Advanced
6 Research Projects Agency, not more than 10 percent may
7 be obligated or expended until the date that is 30 days
8 after the date on which the Under Secretary of Defense
9 for Acquisition, Technology, and Logistics submits to the
10 congressional defense committees a report on how such
11 fund will be managed and executed, including—

12 (1) a concept of operation for how such fund
13 will operate, particularly with regards to supporting
14 the interagency community;

15 (2) a description of—

16 (A) the governance structure, including
17 how decision-making with interagency partners
18 will be conducted;

19 (B) the funding mechanism for interagency
20 collaborators;

21 (C) the metrics for measuring the perform-
22 ance and effectiveness of the program; and

23 (D) the reporting mechanisms to provide
24 oversight of the fund by the Department of De-

1 fense, the interagency partners, and Congress;
2 and
3 (3) any other matters the Under Secretary con-
4 siders appropriate.

1 **SEC. 221 . [Log #235] PROHIBITION ON DELEGATION OF**
2 **BUDGETING AUTHORITY FOR CERTAIN RE-**
3 **SEARCH AND EDUCATIONAL PROGRAMS.**

4 (a) PROHIBITION ON DELEGATION.—Subsection (a)
5 of section 2362 of title 10, United States Code, is amend-
6 ed—

7 (1) by striking "The Secretary of Defense" and
8 inserting "(1) The Secretary of Defense"; and

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

11 "(2) The Secretary of Defense may not delegate to
12 an individual outside the Office of the Secretary of De-
13 fense the authority regarding the programming or budg-
14 eting of the program established by this section that is
15 carried out by the Assistant Secretary of Defense for Re-
16 search and Engineering.".

17 (b) CONFORMING AMENDMENTS.—Such section 2362
18 is amended further—

19 (1) in subsection (b), by striking "established
20 under subsection (a)" and inserting "established by
21 subsection (a)(1)"; and

22 (2) in subsection (c), by striking "subsection
23 (a)" and inserting "subsection (a)(1)".

1 **SEC. 242 _. [Log #159] INDEPENDENT REVIEW AND ASSESS-**
2 **MENT OF CRYPTOGRAPHIC MODERNIZATION**
3 **PROGRAM.**

4 (a) INDEPENDENT REVIEW AND ASSESSMENT.—Not
5 later than 30 days after the date of the enactment of this
6 Act, the Secretary of Defense shall select an appropriate
7 entity outside the Department of Defense to conduct an
8 independent review and assessment of the cryptographic
9 modernization program of the Department of Defense.

10 (b) ELEMENTS.—The review and assessment re-
11 quired by subsection (a) shall include the following:

12 (1) For each military department and appro-
13 priate defense agency, an analysis of the adequacy
14 of the program management structure for executing
15 the cryptographic modernization program, including
16 resources, personnel, requirements generation, and
17 business process metrics.

18 (2) An analysis of the ability of the program to
19 deliver capabilities to the user community while com-
20 plying with the budget and schedule for the pro-
21 gram, including the programmatic risks that nega-
22 tively affect such compliance.

23 (c) REPORT.—

1 (1) REPORT REQUIRED.—Not later than 120
2 days after the date of the enactment of this Act, the
3 entity conducting the review and assessment under
4 subsection (a) shall submit to the Secretary and the
5 congressional defense committees a report con-
6 taining—
7 (A) the results of the review and assess-
8 ment; and
9 (B) recommendations for improving the
10 management of the cryptographic moderniza-
11 tion program.
12 (2) FORM.—The report required by paragraph
13 (1) shall be submitted in unclassified form, but may
14 include a classified annex.

1 **SEC. 251 _. [Log #236] REPEAL OF REQUIREMENT FOR**
2 **TECHNOLOGY TRANSITION INITIATIVE.**
3 (a) IN GENERAL.—
4 (1) REPEAL.—Section 2359a of title 10, United
5 States Code, is repealed.
6 (2) CLERICAL AMENDMENT.—The table of sec-
7 tions at the beginning of chapter 139 of such title
8 is amended by striking the item relating to section
9 2359a.
10 (b) EFFECTIVE DATE.—The amendments made by
11 subsection (a) shall take effect on October 1, 2012.

1 **SEC. 343 . LIMITATION ON OBLIGATION AND EXPENDI-**
2 **TURE OF FUNDS FOR THE MIGRATION OF**
3 **ARMY ENTERPRISE EMAIL SERVICES.**

4 Of the funds authorized to be appropriated by this
5 Act or otherwise made available to the Department of De-
6 fense for fiscal year 2012 for procurement or operation
7 and maintenance for the migration to enterprise email
8 services by the Department of the Army, not more than
9 2 percent may be obligated or expended until the date that
10 is 30 days after the date on which the Secretary of Army
11 submits to the congressional defense committees a report
12 that includes a comparison of the relative merits of
13 transitioning to Defense Information Systems Agency en-
14 terprise email services and Army Knowledge Online. The
15 report shall address each of the following:

16 (1) The original business case analysis sup-
17 porting the decision to transition to Defense Infor-
18 mation Systems Agency enterprise email services.

19 (2) An analysis of alternatives to the decision
20 that were considered.

21 (3) The proposed formal acquisition oversight
22 body and process with respect to the transition.

23 (4) An economic analysis (including a life-cycle
24 cost analysis) of the proposed transition, including a

1 cost-benefit analysis and assessment of sustainment
2 costs.

1 **SEC. 811. [Log #165]. CALCULATION OF TIME PERIOD RE-**
2 **LATING TO REPORT ON CRITICAL CHANGES**
3 **IN MAJOR AUTOMATED INFORMATION SYS-**
4 **TEMS.**

5 Section 2445c(d)(2)(A) of title 10, United States
6 Code, is amended by inserting before the semicolon at the
7 end the following: "after contract award (excluding any
8 time during which the contract award is subject to a bid
9 protest)".

1 **SEC. 901 . [LOG #166] REVISION OF DEFENSE BUSINESS SYS-**
2 **TEMS REQUIREMENTS.**

3 Section 2222 of title 10, United States Code, is
4 amended to read as follows:

5 **"§ 2222. Defense business systems: architecture, ac-**
6 **countability, and modernization**

7 "(a) CONDITIONS FOR OBLIGATION OF FUNDS FOR
8 DEFENSE BUSINESS SYSTEMS.—Funds available to the
9 Department of Defense, whether appropriated or non-ap-
10 propriated, may not be obligated for a defense business
11 system that will have a total cost in excess of $1,000,000
12 unless—

13 "(1) the appropriate pre-certification authority
14 for the defense business system has determined
15 that—

16 "(A) the defense business system is in
17 compliance with the enterprise architecture de-
18 veloped under subsection (c) and appropriate
19 business process re-engineering efforts have
20 been undertaken to ensure that—

21 "(i) the business process to be sup-
22 ported by the defense business system is as
23 streamlined and efficient as practicable;
24 and

"(ii) the need to tailor commercial-off-the-shelf systems to meet unique requirements or incorporate unique requirements or incorporate unique interfaces has been eliminated or reduced to the maximum extent practicable;

"(B) the defense business system is necessary to achieve a critical national security capability or address a critical requirement in an area such as safety or security; or

"(C) the defense business system is necessary to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration the alternative solutions for preventing such adverse effect;

"(2) the defense business system has been reviewed and certified by the investment review board established under subsection (g);

"(3) the certification of the investment review board has been approved by the Defense Business Systems Management Committee established by section 186 of this title.

"(b) OBLIGATION OF FUNDS IN VIOLATION OF REQUIREMENTS.—The obligation of Department of Defense

1 funds for a business system that has not been certified
2 and approved in accordance with subsection (a) is a viola-
3 tion of section 1341(a)(1)(A) of title 31.
4 "(c) ENTERPRISE ARCHITECTURE FOR DEFENSE
5 BUSINESS SYSTEMS.—(1) The Secretary of Defense, act-
6 ing through the Defense Business Systems Management
7 Committee, shall develop—
8 "(A) an enterprise architecture, known as the
9 defense business enterprise architecture, to cover all
10 defense business systems, and the functions and ac-
11 tivities supported by defense business systems, which
12 shall be sufficiently defined to effectively guide, con-
13 strain, and permit implementation of interoperable
14 defense business system solutions and consistent
15 with the policies and procedures established by the
16 Director of the Office of Management and Budget;
17 and
18 "(B) a transition plan for implementing the en-
19 terprise architecture for defense business systems.
20 "(2) The Secretary of Defense shall delegate respon-
21 sibility and accountability for the defense business enter-
22 prise architecture as follows:
23 "(A) The Under Secretary of Defense for Ac-
24 quisition, Technology, and Logistics shall be respon-
25 sible and accountable for the content of those por-

1 tions of the defense business enterprise architecture
2 that support acquisition activities, logistics activities,
3 or installations and environment activities of the De-
4 partment of Defense.

5 "(B) The Under Secretary of Defense (Comp-
6 troller) shall be responsible and accountable for the
7 content of those portions of the defense business en-
8 terprise architecture that support financial manage-
9 ment activities or strategic planning and budgeting
10 activities of the Department of Defense.

11 "(C) The Under Secretary of Defense for Per-
12 sonnel and Readiness shall be responsible and ac-
13 countable for the content of those portions of the de-
14 fense business enterprise architecture that support
15 human resource management activities of the De-
16 partment of Defense.

17 "(D) The Chief Information Officer of the De-
18 partment of Defense shall be responsible and ac-
19 countable for the content of those portions of the de-
20 fense business enterprise architecture that support
21 information technology infrastructure or information
22 assurance activities of the Department of Defense.

23 "(E) The Deputy Chief Management Officer of
24 the Department of Defense shall be responsible and
25 accountable for developing and maintaining the de-

1 fense business enterprise architecture as well as inte-
2 grating business operations covered by subpara-
3 graphs (A) through (D).
4 "(d) COMPOSITION OF ENTERPRISE ARCHITEC-
5 TURE.—The defense business enterprise architecture de-
6 veloped under subsection (c)(1)(A) shall include the fol-
7 lowing:
8 "(1) An information infrastructure that, at a
9 minimum, would enable the Department of Defense
10 to—
11 "(A) comply with applicable law, including
12 Federal accounting, financial management, and
13 reporting requirements;
14 "(B) routinely produce timely, accurate,
15 and reliable business and financial information
16 for management purposes;
17 "(C) integrate budget, accounting, and
18 program information and systems; and
19 "(D) provide for the systematic measure-
20 ment of performance, including the ability to
21 produce timely, relevant, and reliable cost infor-
22 mation.
23 "(2) Policies, procedures, data standards, per-
24 formance measures, and system interface require-

1 ments that are to apply uniformly throughout the
2 Department of Defense.
3 "(3) A defense business systems computing en-
4 vironment integrated into the defense business en-
5 terprise architecture for the major business proc-
6 esses conducted by the Department of Defense, as
7 determined by the Chief Management Officer.
8 "(e) COMPOSITION OF TRANSITION PLAN.—(1) The
9 transition plan developed under subsection (c)(1)(B) shall
10 include the following:
11 "(A) A listing of the additional systems that
12 are expected to be needed to complete the defense
13 business enterprise architecture, along with each
14 system's time-phased milestones, performance meas-
15 ures, financial resource needs, and risks or chal-
16 lenges to integration into the business enterprise ar-
17 chitecture.
18 "(B) A listing of the defense business systems
19 as of December 2, 2002 (known as 'legacy systems'),
20 that will not be part of the defense business enter-
21 prise architecture, together with the schedule for ter-
22 minating those legacy systems that provides for re-
23 ducing the use of those legacy systems in phases.
24 "(C) A listing of the legacy systems (referred to
25 in subparagraph (B)) that will be a part of the de-

1 fense business systems computing environment de-
2 scribed in subsection (d)(3), together with a strategy
3 for making the modifications to those systems that
4 will be needed to ensure that such systems comply
5 with the defense business enterprise architecture.
6 "(2) Each of the strategies under paragraph (1) shall
7 include specific time-phased milestones, performance
8 measures, and a statement of the financial and non-
9 financial resource needs.
10 "(f) APPROPRIATE PRE-CERTIFICATION AUTHORI-
11 TIES.—For purposes of subsection (a), the appropriate
12 pre-certification authority for a defense business system
13 is as follows:
14 "(1) In the case of an Army program, the Chief
15 Management Officer of the Army.
16 "(2) In the case of a Navy program, the Chief
17 Management Officer of the Navy.
18 "(3) In the case of an Air Force program, the
19 Chief Management Officer of the Air Force.
20 "(4) In the case of a program of a Defense
21 Agency, the Director, or equivalent, of that Defense
22 Agency unless otherwise approved by the Deputy
23 Chief Management Officer.
24 "(5) In the case of a program that will support
25 the business processes of more than one military de-

1 partment or Defense Agency, an appropriate pre-cer-
2 tification authority designated by the Deputy Chief
3 Management Officer.
4 "(g) DEFENSE BUSINESS SYSTEM INVESTMENT RE-
5 VIEW.—(1) The Secretary of Defense shall require the
6 Deputy Chief Management Officer, not later than October
7 1, 2011, to establish an investment review board and in-
8 vestment management process, consistent with section
9 11312 of title 40, to review the planning, design, acquisi-
10 tion, development, deployment, operation, maintenance,
11 modernization, and project cost benefits and risks of all
12 defense business systems. The investment review board
13 and investment management process so established shall
14 specifically address the requirements of subsection (a).
15 "(2) The review of defense business systems under
16 the investment management process shall include the fol-
17 lowing:
18 "(A) Review and approval by the investment re-
19 view board of each defense business system before
20 the obligation of funds on the system in accordance
21 with the requirements of subsection (a).
22 "(B) Periodic review, but not less often than
23 annually, of all defense business systems, grouped in
24 portfolios of defense business systems.

1 "(C) Representation on the investment review
2 board by appropriate officials from among the Office
3 of the Secretary of Defense, the armed forces, the
4 combatant commands, the Joint Chiefs of Staff, and
5 the Defense Agencies, including the Under Secre-
6 taries of Defense, the Chief Information Officer of
7 the Department of Defense, and the Chief Manage-
8 ment Officers of the military departments.
9 "(D) Use of threshold criteria to ensure an ap-
10 propriate level of review within the Department of
11 Defense of, and accountability for, defense business
12 systems depending on scope, complexity, and cost.
13 "(E) Use of procedures for making certifi-
14 cations in accordance with the requirements of sub-
15 section (a).
16 "(F) Use of procedures for ensuring consistency
17 with the guidance issued by the Secretary of Defense
18 and the Defense Business Systems Management
19 Committee, as required by section 186(c) of this
20 title, and incorporation of common decision criteria,
21 including standards, requirements, and priorities
22 that result in the integration of defense business sys-
23 tems.
24 "(h) BUDGET INFORMATION.—In the materials that
25 the Secretary submits to Congress in support of the budg-

1 et submitted to Congress under section 1105 of title 31
2 for fiscal year 2006 and fiscal years thereafter, the Sec-
3 retary of Defense shall include the following information:
4 "(1) Identification of each defense business sys-
5 tem for which funding is proposed in that budget.
6 "(2) Identification of all funds, by appropria-
7 tion, proposed in that budget for each such system,
8 including—
9 "(A) funds for current services (to operate
10 and maintain the system); and
11 "(B) funds for business systems mod-
12 ernization, identified for each specific appro-
13 priation.
14 "(3) For each such system, identification of the
15 appropriate pre-certification authority under sub-
16 section (f).
17 "(4) For each such system, a description of
18 each approval made under subsection (a)(3) with re-
19 gard to such system.
20 "(i) CONGRESSIONAL REPORTS.—Not later than
21 March 15 of each year from 2012 through 2016, the Sec-
22 retary of Defense shall submit to the congressional defense
23 committees a report on Department of Defense compliance
24 with the requirements of this section. The report shall—

1 "(1) describe actions taken and planned for
2 meeting the requirements of subsection (a), includ-
3 ing—
4 "(A) specific milestones and actual per-
5 formance against specified performance meas-
6 ures, and any revision of such milestones and
7 performance measures; and
8 "(B) specific actions on the defense busi-
9 ness systems submitted for certification under
10 such subsection;
11 "(2) identify the number of defense business
12 systems so certified;
13 "(3) identify any defense business system dur-
14 ing the preceding fiscal year that was not certified
15 under subsection (a), and the reasons for the lack of
16 certification;
17 "(4) discuss specific improvements in business
18 operations and cost savings resulting from successful
19 defense business systems implementation or mod-
20 ernization efforts; and
21 "(5) include a copy of the most recent report of
22 the Chief Management Officer of each military de-
23 partment on implementation of business trans-
24 formation initiatives by such department in accord-
25 ance with section 908 of the Duncan Hunter Na-

1 tional Defense Authorization Act for Fiscal Year
2 2009 (Public Law 110–417; 122 Stat. 4569; 10
3 U.S.C. 2222 note).
4 "(j) DEFINITIONS.—In this section:
5 "(1) The term 'pre-certification authority', with
6 respect to a defense business system, means the De-
7 partment of Defense official responsible for the de-
8 fense business system, as designated by subsection
9 (f).
10 "(2) The term 'defense business system' means
11 an information system, other than a national secu-
12 rity system, operated by, for, or on behalf of the De-
13 partment of Defense, including financial systems,
14 mixed systems, financial data feeder systems, and
15 information technology and information assurance
16 infrastructure, used to support business activities,
17 such as acquisition, financial management, logistics,
18 strategic planning and budgeting, installations and
19 environment, and human resource management.
20 "(3) The term 'enterprise architecture' has the
21 meaning given that term in section 3601(4) of title
22 44.
23 "(4) The terms 'information system' and 'infor-
24 mation technology' have the meanings given those
25 terms in section 11101 of title 40.

1 "(5) The term 'national security system' has
2 the meaning given that term in section 3542(b)(2)
3 of title 44.".

1 **SEC. 963 [Log #240]. ACTIVITIES TO IMPROVE MULTILAT-**
2 **ERAL, BILATERAL, AND REGIONAL COOPERA-**
3 **TION REGARDING CYBERSECURITY.**

4 (a) ESTABLISHMENT OF CYBERSECURITY PRO-
5 GRAM.—

6 (1) IN GENERAL.—Chapter 53 of title 10,
7 United States Code, is amended by inserting after
8 section 1051b the following new section:

9 **"§ 1051c. Multilateral, bilateral, or regional coopera-**
10 **tion programs: assignments to improve**
11 **education and training in information se-**
12 **curity**

13 "(a) ASSIGNMENTS AUTHORIZED; PURPOSE.—The
14 Secretary of Defense may authorize the temporary assign-
15 ment of a member of the military forces of a foreign coun-
16 try to a Department of Defense organization for the pur-
17 pose of assisting the member to obtain education and
18 training to improve the member's ability to understand
19 and respond to information security threats,
20 vulnerabilities of information security systems, and the
21 consequences of information security incidents.

22 "(b) PAYMENT OF CERTAIN EXPENSES.—To facili-
23 tate the assignment of a member of a foreign military
24 force to a Department of Defense organization under sub-

1 section (a), the Secretary of Defense may pay such ex-
2 penses in connection with the assignment as the Secretary
3 considers in the national security interests of the United
4 States.

5 "(c) PROTECTION OF DEPARTMENT
6 CYBERSECURITY.—In authorizing the temporary assign-
7 ment of members of foreign military forces to Department
8 of Defense organizations under subsection (a), the Sec-
9 retary of Defense shall require the inclusion of adequate
10 safeguards to prevent any compromising of Department
11 information security.

12 "(d) MULTI-YEAR AVAILABILITY OF FUNDS.—Funds
13 available to carry out this section shall be available, to the
14 extent provided in appropriations Acts, for programs and
15 activities under this section that begin in a fiscal year and
16 end in the following fiscal year.

17 "(e) INFORMATION SECURITY DEFINED.—In this
18 section, the term 'information security' refers to—

19 "(1) the confidentiality, integrity, or availability
20 of an information system or the information such
21 system processes, stores, or transmits; and

22 "(2) the security policies, security procedures,
23 or acceptable use policies with respect to an informa-
24 tion system.".

1 (2) CLERICAL AMENDMENT.—The table of sec-
2 tions at the beginning of such chapter is amended
3 by inserting after the item relating to section 1051b
4 the following new item:

"1051c. Multilateral, bilateral, or regional cooperation programs: assignments to improve education and training in information security.".

5 (b) REPORT ON EXPANSION OF FELLOWSHIP OPPOR-
6 TUNITIES.—Not later one year after the date of the enact-
7 ment of this Act, the Secretary of Defense shall submit
8 to Congress a report evaluating the feasibility and benefits
9 of expanding the fellowship program authorized by section
10 1051c of title 10, United States Code, as added by sub-
11 section (a), to include ministry of defense officials, secu-
12 rity officials, or other civilian officials of foreign countries.

1 **SEC. 964. REPORT ON UNITED STATES SPECIAL OPER-**
2 **ATIONS COMMAND STRUCTURE.**

3 (a) REPORT.—Not later than March 1, 2012, the
4 Secretary of Defense shall submit to the congressional de-
5 fense committees a study of the United States Special Op-
6 erations Command sub-unified structure.

7 (b) ELEMENTS.—The report required under this sec-
8 tion shall include, at a minimum, the following:

9 (1) Recommendations to revise as necessary the
10 present command structure to better support devel-
11 opment and deployment of joint special operations
12 forces and capabilities.

13 (2) Any other matters the Secretary considers
14 appropriate.

15 (c) FORM.—The report required under this section
16 shall be submitted in unclassified form, but may include
17 a classified annex.

1 **SEC. 1032 . EXTENSION OF AUTHORITY TO MAKE REWARDS**
2 **FOR COMBATING TERRORISM.**

3 Section 127b of title 10, United States Code, is
4 amended—

5 (1) in subsection (c)(3)(C), by striking "Sep-
6 tember 30, 2011" and inserting "September 30,
7 2014"; and

8 (2) in subsection (f)(1), by striking "Decem-
9 ber" and inserting "February".

1 **SEC. 1041 . COUNTERTERRORISM OPERATIONAL BRIEFING**
2 **REQUIREMENT.**

3 (a) BRIEFINGS REQUIRED.—Beginning not later
4 than March 1, 2012, the Secretary of Defense shall pro-
5 vide to the congressional defense committees quarterly
6 briefings outlining Department counterterrorism oper-
7 ations and related activities involving special operations
8 forces.

9 (b) ELEMENTS.—Each briefing under subsection (a)
10 shall include each of the following:

11 (1) A global update on activity within each geo-
12 graphic combatant command.

13 (2) An overview of authorities and legal issues
14 including limitations.

15 (3) An outline of interagency activities and ini-
16 tiatives.

17 (4) Any other matters the Secretary considers
18 appropriate.

1 **SEC. 1077 . ASSESSMENT OF THE DEFENSE INDUSTRIAL**
2 **BASE PILOT PROGRAM.**

3 (a) REPORT.—Not later than March 1, 2012, the
4 Secretary of Defense shall submit to the congressional de-
5 fense committees a report on the defense industrial base
6 pilot program of the Department of Defense.

7 (b) ELEMENTS.—The report required by subsection
8 (a) shall include each of the following:

9 (1) A quantitative and qualitative analysis of
10 the effectiveness of the defense industrial base pilot
11 program.

12 (2) An assessment of the legal, policy, or regu-
13 latory challenges associated with effectively exe-
14 cuting the pilot program.

15 (3) Recommendations for changes to the legal,
16 policy, or regulatory framework for the pilot pro-
17 gram to make it more effective.

18 (4) A description of any plans to expand the
19 pilot program, including to other sectors beyond the
20 defense industrial base.

21 (5) An assessment of the potential legal, policy,
22 or regulatory challenges associated with expanding
23 the pilot program.

1 (6) Any other matters the Secretary considers
2 appropriate.
3 (c) FORM.—The report required under this section
4 shall be submitted in unclassified form, but may include
5 a classified annex.

1 **SEC. 1092 . [Log #243] TREATMENT UNDER FREEDOM OF IN-**
2 **FORMATION ACT OF CERTAIN DEPARTMENT**
3 **OF DEFENSE CRITICAL INFRASTRUCTURE IN-**
4 **FORMATION.**

5 (a) IN GENERAL.—Chapter 3 of title 10, United
6 States Code, is amended by adding at the end the fol-
7 lowing new section:

8 **"§ 130e. Treatment under Freedom of Information**
9 **Act of critical infrastructure information**

10 "(a) EXEMPTION.—Department of Defense critical
11 infrastructure information that, if disclosed, may result in
12 the disruption, degradation, or destruction of operations,
13 property, or facilities of the Department of Defense, shall
14 be exempt from disclosure pursuant to section 552(b)(3)
15 of title 5.

16 "(b) INFORMATION PROVIDED TO STATE AND LOCAL
17 GOVERNMENTS.—Department of Defense critical infra-
18 structure information obtained by a State or local govern-
19 ment from a Federal agency shall remain under the con-
20 trol of the Federal agency, and a State or local law author-
21 izing or requiring such a government to disclose informa-
22 tion shall not apply to such critical infrastructure informa-
23 tion.

1 "(c) REGULATIONS.—The Secretary of Defense shall
2 prescribe regulations to implement this section.".
3 (b) CLERICAL AMENDMENT.—The table of sections
4 at the beginning of such chapter is amended by adding
5 at the end the following new item:

"130e. Treatment under Freedom of Information Act of certain critical infrastructure information.".

1 **SEC. 1093 [Log #30]. EXPANSION OF SCOPE OF HUMANI-**
2 **TARIAN DEMINING ASSISTANCE PROGRAM**
3 **TO INCLUDE STOCKPILED CONVENTIONAL**
4 **MUNITIONS ASSISTANCE.**

5 Section 407 of title 10, United States Code, is
6 amended—

7 (1) in subsection (a)—

8 (A) in paragraph (1), by inserting "and
9 stockpiled conventional munitions assistance"
10 after "demining assistance"; and

11 (B) in paragraph (3)(A), by inserting ",
12 stockpiled conventional munitions," after "land-
13 mines";

14 (2) in subsection (d)(2), by inserting ", and
15 whether such assistance was primarily related to the
16 humanitarian demining efforts or stockpiled conven-
17 tional munitions assistance" after "paragraph (1)";
18 and

19 (3) by striking subsection (e) and inserting the
20 following new subsection (e):

21 "(e) DEFINITIONS.—In this section:

22 "(1) The term 'humanitarian demining assist-
23 ance', as it relates to training and support, means
24 detection and clearance of landmines and other ex-
25 plosive remnants of war, and includes activities re-
26 lated to the furnishing of education, training, and

1 technical assistance with respect to explosive safety,
2 the detection and clearance of landmines and other
3 explosive remnants of war, and the disposal, demili-
4 tarization, physical security, and stockpile manage-
5 ment of potentially dangerous stockpiles of explosive
6 ordnance.

7 "(2) The term 'stockpiled conventional muni-
8 tions assistance', as it relates to the support of hu-
9 manitarian assistance efforts, means training and
10 support in the disposal, demilitarization, physical se-
11 curity, and stockpile management of potentially dan-
12 gerous stockpiles of explosive ordnance, and includes
13 activities related to the furnishing of education,
14 training, and technical assistance with respect to ex-
15 plosive safety, the detection and clearance of land-
16 mines and other explosive remnants of war, and the
17 disposal, demilitarization, physical security, and
18 stockpile management of potentially dangerous
19 stockpiles of explosive ordnance.".

1 **SEC. 1201. EXPANSION OF AUTHORITY FOR SUPPORT OF**
2 **SPECIAL OPERATIONS TO COMBAT TER-**
3 **RORISM.**

4 (a) AUTHORITY.—Subsection (a) of section 1208 of
5 the Ronald W. Reagan National Defense Authorization
6 Act for Fiscal Year 2005 (Public Law 108–375; 118
7 Stat.2086), as most recently amended by section 1201 of
8 the Ike Skelton National Defense Authorization Act for
9 Fiscal Year 2011 (Public Law 111–383; 124 Stat. 4385),
10 is further amended by striking "$45,000,000" and insert-
11 ing "$50,000,000".

12 (b) EXTENSION.—Subsection (h) of such section, as
13 most recently amended by section 1208(c) of the Duncan
14 Hunter National Defense Authorization Act for Fiscal
15 Year 2009 (Public Law 110–417; 122 Stat. 4626), is fur-
16 ther amended by striking "2013" and inserting "2014".

17 (c) BRIEFING AND REPORT.—Not later than 90 days
18 after the date of the enactment of this Act, the Secretary
19 of Defense shall provide to the Committees on Armed
20 Services of the Senate and House of Representatives a
21 briefing and a report that outlines future requirements for
22 the authorities contained in section 1208 of the Ronald
23 W. Reagan National Defense Authorization Act for Fiscal
24 Year 2005 (Public Law 108–375; 118 Stat.2086) (as

1 amended by this section), authorities similar to the au-
2 thorities contained in section 1208 of such Act, and au-
3 thorities to support special operations counterterrorism,
4 unconventional warfare, and irregular warfare in anticipa-
5 tion of and preparation for the expiration of the authori-
6 ties under section 1208 of such Act at the end of fiscal
7 year 2014.

1 **SEC. 1204 . FIVE-YEAR EXTENSION OF AUTHORIZATION**
2 **FOR NON-CONVENTIONAL ASSISTED RECOV-**
3 **ERY CAPABILITIES.**

4 Section 943(h) of the Duncan Hunter National De-
5 fense Authorization Act for Fiscal Year 2009 (Public Law
6 110–417; 122 State. 4579) is amended by striking
7 "2011" and inserting "2016".

1 **SEC. 1404 [Log #___]. CHEMICAL AGENTS AND MUNITIONS**
2 **DESTRUCTION, DEFENSE.**

3 (a) AUTHORIZATION OF APPROPRIATIONS.—Funds
4 are hereby authorized to be appropriated for the Depart-
5 ment of Defense for fiscal year 2012 for expenses, not oth-
6 erwise provided for, for Chemical Agents and Munitions
7 Destruction, Defense, as specified in the funding table in
8 section 4501.

9 (b) USE.—Amounts authorized to be appropriated
10 under subsection (a) are authorized for—

11 (1) the destruction of lethal chemical agents
12 and munitions in accordance with section 1412 of
13 the Department of Defense Authorization Act, 1986
14 (50 U.S.C. 1521); and

15 (2) the destruction of chemical warfare materiel
16 of the United States that is not covered by section
17 1412 of such Act.

1 **SEC. 1421 . CHANGES TO MANAGEMENT ORGANIZATION TO**
2 **THE ASSEMBLED CHEMICAL WEAPONS AL-**
3 **TERNATIVE PROGRAM.**

4 (a) MANAGEMENT ORGANIZATION.—Section
5 1412(g)(2) of the Department of Defense Authorization
6 Act, 1986 (50 U.S.C. 1521) is amended by striking the
7 last sentence.

8 (b) BRIEFING REQUIRED.—Not later than 60 days
9 after the date of the enactment of this Act, the Assistant
10 Secretary of Defense for Nuclear, Chemical, and Biologi-
11 cal Defense Programs, in coordination with the Deputy
12 Assistant Secretary of the Army for the Elimination of
13 Chemical Weapons, shall provide to Committees on Armed
14 Services of the Senate and House of Representatives a
15 briefing on opportunities to leverage lessons learned and
16 experienced personnel of the Army Chemical Materials
17 Agency to support the Assembled Chemical Weapons Al-
18 ternatives program. The briefing shall include each of the
19 following:

20 (1) A plan to attract Army Chemical Materials
21 Agency personnel to assist the Assembled Chemical
22 Weapons Alternatives program in completing the
23 mission of the Agency set forth by the Chemical
24 Weapons Convention and the destruction of the

1 United States' stockpile of lethal chemical agents
2 and munitions by the deadline under section 1412 of
3 the Department of Defense Authorization Act, 1986
4 (50 U.S.C. 1521), and an analysis of that plan.
5 (2) An analysis of how the Army Chemical Ma-
6 terials Agency and the Assembled Chemical Weap-
7 ons Alternative program can work in coordination to
8 ensure that the leadership, expertise, experience, and
9 best practices of the Agency are shared extensively
10 with the Assembled Chemical Weapons Alternative
11 program.
12 (3) An analysis of how the Assembled Chemical
13 Weapons Alternative program could incorporate best
14 practices from the Army Chemical Materials Agency.
15 (c) DEFINITION.—The term "Chemical Weapons
16 Convention" means the Convention on the Prohibition of
17 the Development, Production, Stockpiling and Use of
18 Chemical Weapons and on Their Destruction, ratified by
19 the United States on April 25, 1997, and entered into
20 force on April 29, 1997.

SUMMARY OF DIRECTIVE REPORT LANGUAGE

Titles 2, 7, 9, & 10

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

3-D advanced integrated circuit capabilities

Cyber test and evaluation

Defense laboratory survey

Medical Countermeasures Initiative and the chemical and biological defense program

Mobile applications development

Nanotechnology research

Project Pelican

University affiliated research centers

TITLE VII—HEALTH CARE PROVISIONS

Use of Simulation Technology in Medical Training

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

Office of Cyberthreat Analysis

TITLE X—GENERAL PROVISIONS

Countering Adversarial Narratives

Countering Network-Based Threats

Cyber Threats to Critical Infrastructure

Economic Warfare

Planning for Electromagnetic Pulse Events

The Role of Military Information Support Operations

DIRECTIVE REPORT LANGUAGE

Titles 2, 7, 9, & 10

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

3-D advanced integrated circuit capabilities

The committee is concerned about the domestic capacity to produce 3-D advanced integrated circuits in the United States. The committee is aware that much of the commercial capacity has been moved offshore, making the global supplier base for defense microelectronics increasingly insecure and susceptible to compromise through counterfeit or maliciously-altered circuits.

Therefore, the committee directs the Secretary of Defense to conduct a comprehensive assessment regarding 3-D integrated circuits manufacturing capacity to serve the U.S. military and other national security interests and to provide a report on the findings to the Senate Committee on Armed Services and the House Committee on Armed Services within 90 days after the date of the enactment of this Act. The report should include the following:

(1) An assessment of the military requirements for 3-D integrated circuits in future microelectronic systems as a critical enabling technology for military applications;

(2) An assessment of the current domestic commercial capability to securely develop and manufacture 3-D integrated circuits for use in military systems and;

(3) An assessment of the feasibility, as well as planning and design requirements, for the development of a domestic manufacturing capability for 3-D integrated circuits at a number of locations within the United States, including Fort Leonard Wood, Missouri.

Cyber test and evaluation

The committee recognizes the importance of information technology (IT) and cyber security-related technologies in providing critical capabilities to Armed Forces in the future. The Weapon Systems Acquisition Reform Act of 2009 (Public Law 111-23) and the report "Panel on Defense Acquisition Reform Findings and Recommendations" places significant importance on conducting rigorous testing and evaluation in order to improve defense acquisition outcomes. While the "2010 Test and Evaluation Strategic Plan" addresses numerous capability gaps in cyber testing, the committee is concerned that the Department of Defense is not providing sufficient resources to address rapidly increasing demands to conduct developmental and operational test and evaluation (T&E) for future IT systems.

Therefore, the committee directs the Under Secretary of Defense for Acquisition, Technology, and Logistics , in coordination with the Secretaries of the military departments, to conduct an analysis of T&E resources needed to address the capability gaps outlined by the "2010 Test and Evaluation Strategic Plan." The analysis should examine the following:

(1) Whether the Department of Defense is sufficiently funding T&E at the level necessary to address cyber and IT capability needs over the Future Years Defense Program;

(2) Whether the Department of Defense has sufficient numbers of technical personnel with the expertise in IT disciplines to conduct T&E for cyber and IT systems over the Future Years Defense Program; and

(3) Whether the Department of Defense has adequate infrastructure to conduct T&E for cyber and IT systems over the Future Years Defense Program.

The committee further directs the Under Secretary of Defense for Acquisition, Technology, and Logistics to brief the Senate Committee on Armed Services and the House Committee on Armed Services on the results of this analysis within 180 days after date of the enactment of this Act.

Defense laboratory survey

The committee recognizes the key role that Department of Defense (DOD) laboratories play in technology development, scientific innovation, and acquisition excellence. DOD laboratories are critical to maintaining the technological superiority and competency of the military, and to monitor global technology developments to prevent surprise and mitigate adversarial developments. The committee remains committed to ensuring that the Department of Defense laboratory system has the resources and authority to support the scientific and technological management of the military.

The committee is concerned, however, that there may be certain regulations, instructions, policies and practices instituted by the Department and the military services that may lessen the laboratories effectiveness and efficiency, hindering the innovative spirit that drives the laboratories. The committee believes that an assessment of the possible constraints on the mission of the various laboratories would be beneficial to ensuring their long-term viability as leaders in the pursuit of technological advancement.

Therefore, the committee directs the Assistant Secretary of Defense for Research and Engineering to survey directors of the Department of Defense laboratories to determine how to streamline DOD regulations, instructions and policies impacting the laboratories and to make recommendations to improve the Department of Defense laboratory system. The committee further directs the Assistant Secretary of Defense for Research and Engineering to provide a briefing on the results of this survey to the Senate Committee on Armed Services and House Armed Services Committee within 120 days after the date of enactment of this Act.

Medical Countermeasures Initiative and the chemical and biological defense program

The committee is aware that the Department of Defense is pursuing a new Medical Countermeasure Initiative (MCMI) within the chemical and biological defense program designed to enable rapid delivery of new medical countermeasures to dangerous pathogens through a strategic partnership between the U.S. Government and industry. The committee is also aware that MCMI is designed to enhance force protection for military personnel against emerging threats and infectious diseases and fill a capability gap, which was underscored by the inability to rapidly produce vaccine for the 2009 H1N1 influenza virus pandemic.

The committee is also aware that the Government Accountability Office (GAO) recently reported in GAO-11-318SP "Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue" that most Federal efforts and programs within the bio-defense enterprise are fragmented and that the overarching enterprise lacks strategic oversight mechanisms. GAO also concludes that there is no broad, integrated national strategy that encompasses all stakeholders with bio-defense responsibilities that can be used to guide the systemic identification of risk, assessment of resources needed to address those risks, and the prioritization and allocation of investment across the entire Federal Government. As such, neither the Office of Management and Budget, nor the Federal agencies account for bio-defense spending across the entire Federal Government.

While the committee understands the need to ensure rapid delivery of advanced medical countermeasures to dangerous pathogens, the committee is concerned that the Department is initiating MCMI as a new-start program in a bio-defense sector already identified by GAO as fragmented and disjointed. The committee therefore directs the Secretary of Defense to provide a detailed briefing to the Senate Committee on Armed Services and the House Committee on Armed Services within 90 days after the date of enactment of this Act, on the efforts taken by the Department to ensure programmatic success in this area, including but not limited to: cost, schedule, and performance in the Future Years Defense Program; efforts to interface with and implement cost-sharing mechanisms across industry; efforts to enhance efficiencies and reduce fragmentation related to Department of Defense equities within the interagency bio-defense enterprise; and efforts taken to ensure interagency collaboration such as cross-cutting information management and communications, research and development, and acquisition efforts.

Mobile applications development

The committee is aware that the military departments and Defense agencies are pursuing future network strategies that would leverage developments in the commercial marketplace. These commercially-developed mobile devices, such as smart phones and tablet computers, are in high demand by the Armed Forces, and offer computational power, flexibility, and technology refresh rates not currently achievable in military-developed communications and computing devices.

The committee is also aware that some defense organizations, such as the Army, the Defense Information Systems Agency, and the Defense Advanced Research Projects Agency (DARPA), have begun experimenting with mobile computing devices to field relevant applications for military use. For example, the Army held a competition in 2010 to spur development of mobile device applications, and has established a small, dedicated effort within Training and Doctrine Command to focus on mobile applications development. DARPA has also begun examining how the Department might support applications development for mobile computing devices in the future.

The committee is concerned that the Department has not devoted sufficient attention to these efforts, and thus the necessary policy developments needed to support these technology developments has been lagging. For example, the process for test, evaluation, certification and accreditation of these applications for network use has not been sufficiently clarified and takes significantly longer than similar processes in the commercial sector. This time lag and policy ambiguity has resulted in some users bypassing security procedures in order to get access to the capabilities these applications provide.

Therefore, the committee directs the Department of Defense (DOD) Chief Information Officer to develop and issue a Department of Defense Instruction within 180 days after the date of enactment of this Act to clarify the process for developing and using mobile applications on DOD networks. The Instruction should address development, test, evaluation, certification, accreditation, and mechanisms for making these applications available to the user community. The development of the Instruction should also be coordinated through the working group process supporting the development of a rapid information technology acquisition process as part of section 804 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111-84).

Nanotechnology research

The committee is aware that the Department of Defense is pursuing research into a variety of nanotechnology applications for defense purposes. New capabilities enabled by the unique performance enhancements of nanostructured materials hold the potential of transforming the technology landscape. The committee encourages the Department to continue to make investments in nanotechnology research that is needed to create the next generation of sensors, electronics, weapons, and manufacturing processes.

However, the committee is concerned that the Department of Defense lacks sufficient expertise in some emerging research disciplines related to nanotechnology to support a long-term research investment strategy. The committee is aware that a dedicated federally funded research and development center (FFRDC) could support the Department in this effort, but that no such broad-based nanotechnology FFRDC exists.

Therefore, the committee directs the Assistant Secretary of Defense for Research and Engineering to provide a report to the Senate Committee on Armed Services and the House Committee on Armed Services within 90 days after the date of enactment of this Act on how the Department of Defense receives support from the research community on nanotechnology issues, including identifying of where within the existing FFRDC community that expertise comes from, and assessing whether a dedicated FFRDC is needed.

Project Pelican

The committee continues to support the efforts within the Office of the Assistant Secretary of Defense for Research and Engineering to pursue a technology demonstrator for a rigid-hull, variable-buoyancy hybrid air vehicle, known as "Project Pelican." As noted in the committee report (H. Rept. 111-166) accompanying the National Defense Authorization Act for Fiscal Year 2010, the proposed capabilities have the potential to revolutionize the future of intra-theater lift, as well as other areas of importance, such as intelligence, surveillance, reconnaissance, and communications relay.

However, the committee is cautiously optimistic about the progress of the demonstrator vehicle, and cautions against scaling this vehicle up to an operational system before the technology is adequately validated. The committee is concerned that airship technology has a history of being hampered by a variety of operational constraints that the military has not adequately dealt with since the last military airships were retired more than 50-years ago. The committee believes the Department should pursue a parallel path that demonstrates robust concepts of operation as the technology is matured and validated. Part of the process of developing concepts of operation should include planning and analysis for addressing operational and logistical constraints of using large airships, such as basing, airspace management, and environmental issues.

Therefore, the committee directs the Assistant Secretary of Defense for Research and Engineering to conduct a series of tabletop exercises, in conjunction with the service acquisition executives of the military departments and the combatant commanders, to develop concepts of operations for how rigid-hull, variable-buoyancy hybrid air vehicle technology might be employed in future platforms. The committee further directs the Assistant Secretary to brief the Senate Committee on Armed Services and the House Committee on Armed Services on the results of the tabletop exercises within 270 days after the date of enactment of this Act.

University affiliated research centers

The committee is aware that the Department of Defense funds a number of university affiliated research centers (UARC) to support its research needs. Although permitted by law to award research and development contracts non-

competitively to only universities and other non-profit organizations, the Department of Defense has chosen to limit the UARC program to universities. The committee is concerned that by barring them from programs such as UARCs, the Department is depriving itself from utilizing specialized expertise that exists within non-profit research and development organizations.

Therefore, the committee directs the Assistant Secretary of Defense for Research and Engineering to review the Department of Defense's guidance pertaining to non-profit research institutions to participate in UARCs and other research and development contracting opportunities to ensure that these organizations are not being unfairly excluded from competitions. The committee further directs the Assistant Secretary of Defense for Research and Engineering to provide a briefing on the results of this review to the Senate Committee on Armed Services and House Committee on Armed Services within 90 days after the date of enactment of this Act.

TITLE VII—HEALTH CARE PROVISIONS

Use of Simulation Technology in Medical Training

The committee is aware that the Department of Defense (DOD) currently supplements combat trauma training with the use of live animals, known as "live tissue training", when no suitable simulation technology or alternative exists. The committee notes that this advanced training has contributed directly to the high survival rate for combat wounded service members, which has increased significantly compared to survival rates in past conflicts. According to the Department, simulators currently lack sufficient realism and the ability to replicate combat wounds and the associated emotional stressors combat medics face on the battlefield. In addition, simulators require rigorous verification and validation, which can only be achieved through empirical data collection. The committee also notes that the Department's use of live tissue training is strictly regulated by a number of Federal laws and policies, and is accredited by the Association for the Assessment and Accreditation of Laboratory Animal Care, an international non-profit organization that promotes the humane use of animals in science.

On September 5, 2008, the Under Secretary of Defense for Acquisition, Technology, and Logistics established the Use of Live Animals in Medical Education and Training Joint Analysis Team (ULAMET JAT) to address the use of live animals for DOD medical readiness training. ULAMET JAT, in its final report, found that several critical, high stakes medical procedures cannot be taught at present using simulation, including the treatment of certain penetrating chest wounds, amputation, and hemostasis. ULAMET JAT further noted in its final report that "live animal training is the singular opportunity to experience management of injuries in a living system prior to deployment to a combat zone. The next opportunity to use these skills very likely will be treating combat wounded." ULAMET JAT's final report also made nine recommendations related to

the Department's policies on the use of animals in combat trauma training and plans to validate and adopt alternatives as they become viable, including simulation technologies.

The committee believes that the use of animals in combat trauma training remains appropriate for critical, high-risk medical procedures, until such time that alternatives are developed, to provide combat medics an equal or better training experience that more closely replicates the combat wounds and emotional stressors encountered on the battlefield. However, the committee believes that the Department should continue to aggressively pursue alternatives to the use of live animals in combat trauma training.

Therefore, the committee directs the Secretary of Defense to finalize and implement a strategy for the development of future technology to further refine, reduce, and replace the use of live animals in medical education and training. This implementation strategy should leverage the Department's science and technology and research, development, testing, and evaluation organizations, as well as private industry, to develop additional advanced training simulators and training aids, including animal-alternative training, to offer the most realistic, practical, transferable, and cost-effective training to all medical personnel. The Secretary is further directed to provide a briefing to the Senate Committee on Armed Services and the House Committee on Armed Services within 90 days after the date of enactment of this Act, on this implementation strategy and the status of the recommendations contained within ULAMET JAT's final report.

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

Office of Cyberthreat Analysis

The committee is aware that the Defense Intelligence Agency has established the Office of Cyberthreat Analysis to provide an all-source analysis capability focused on threats in cyberspace. The office provides a range of support functions to the entire defense community, including: all-source defense analysis of cyberthreats to the Nation; target development; exercise planning;battle damage assessment; and counterintelligence investigations and operations, including supply chain risk management.

The committee is concerned that this office has not been sufficiently staffed to complete the tasks assigned. For instance, the growing importance of conducting supply chain risk assessments and vulnerability assessments on specific acquisition programs are likely to drive the needs for the limited numbers of personnel, making it difficult to carry out other missions. Therefore, the committee directs the Under Secretary of Defense for Intelligence, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Commander, U.S. Cyber Command to assess the sufficiency of the workforce assigned to the Office of Cyberthreat Analysis compared to the missions assigned to it. The Under Secretary

of Defense for Intelligence shall submit a report on this assessment to the Senate Committee on Armed Services and the House Committee on Armed Services by 90 days after the enactment of this Act.

TITLE X—GENERAL PROVISIONS

Countering Adversarial Narratives

The committee applauds the U.S. Government, and in particular the Department of Defense, for its efforts to develop and implement an effective communications strategy to counter violent extremist messaging and other adversarial narratives. However, the committee remains concerned that the United States and its allies are losing the ever present information campaign to its adversaries. Through the use of emerging new media capabilities, our enemies make it appear that they are acting more swiftly and with a more unified message than the U.S. Government. Furthermore, many of these media channels originate in the United States or neutral countries and pose an even greater challenge because they threaten our ability to successfully communicate our objectives while negating our ability to counter their information flow.

The committee is concerned that the Armed Forces are increasingly seen as the strategic communications provider for the United States within their areas of responsibilities. The committee is concerned, though, that the Department is increasingly challenged by a shortage of in-house practical expertise and, in general, military and civilian senior leadership has limited or no practical experience in strategic communication. The committee is also concerned that the Department lacks the technical capabilities to respond in a systemic, rapid, sustained and measurable way to the constant barrage of narratives being used to undermine our military and security efforts.

Therefore, the committee directs the Secretary of Defense to conduct an assessment of the Department of Defense's efforts to counter adversarial narratives and provide a briefing on the findings to the Senate Committee on Armed Services and the House Committee on Armed Services within 150 days after the date of enactment of this Act. This assessment should address the following:

(1) Does the Department of Defense have the authorities, organizational structure, tools, techniques, procedures, and resources to rapidly analyze and respond to adversarial narratives in the information environment;

(2) Does the Department of Defense have adequate manpower, talent pool and training base to provide the leadership and staffing required to monitor and respond to adversarial narratives in the information environment; and

(3) What additional legal authorities or resources are necessary to remedy any challenges or shortages that limit the Department's ability to succeed.

Countering Network-Based Threats

The committee continues to encourage the Secretary of Defense to pursue efforts to develop innovative, non-materiel, and multi-disciplinary methodologies and strategies for disrupting irregular and asymmetric threats. During his March 2011 Senate confirmation hearing, the Under Secretary of Defense for Intelligence testified that "a comprehensive understanding of the socio-cultural environment is absolutely critical to developing and implementing effective strategies to separate the insurgency from any viable base of support in the general population," and that "a detailed understanding of tribal dynamics is a critical intelligence task, and will likely remain so for the foreseeable future." The committee believes an effective military strategy for operations, such as those in the Islamic Republic of Afghanistan, must appropriately balance kinetic operations with counterinsurgency operations, emphasizing population protection, tribal dynamics, cultural insight, and the rule of law. However the committee remains concerned that the intelligence community is overwhelmingly focused on kinetic operations to the detriment of the socio-cultural environment critical to counterinsurgency operations.

The committee notes that U.S. Army Field Manual 3-24, dated December 2006, defines the key to all counterinsurgency tasks is developing an effective host-nation security force. Chapter 6 of the manual states: "Few military units can match a good police unit in developing an accurate human intelligence picture of their area of operation. Because of their frequent contact with populace, police often are the best force for countering small insurgent bands supported by the local populace."

The committee remains concerned that the Secretary of Defense has not taken full advantage of a novel approach that takes into account an understanding of the tribal landscape and invests in developing host-nation security forces, particularly local police organizations that maintain close ties with and function to protect the local population. The committee praised this approach, the Legacy program, in the committee report (H. Rept. 111-491) accompanying the National Defense Authorization Act for Fiscal Year 2011. In the report, the committee noted special interest in the "Attack the Network" approach used in the Republic of Iraq and Afghanistan under the Legacy program.

Accordingly, the committee directs the Secretary of Defense to conduct an assessment of the following:

(1) The applicability of the Legacy program in other operations and regions where network-based threats are present or where conditions are conducive to supporting these threats; and

(2) Options for an appropriate management structure within the Department to institutionalize and sustain the capabilities that Legacy and other similar programs provide.

The committee further directs the Secretary of Defense to brief the Senate Committee on Armed Services and the House Committee on Armed Services, by July 31, 2011, on the findings of the aforementioned activities and on the plan in H.

Rept. 111-491 for supporting and sustaining innovative approaches, including such approaches that incorporate and blend legal, law enforcement, intelligence, and military tactics, techniques, and procedures.

Cyber Threats to Critical Infrastructure

The committee is aware of the Department of Defense's efforts to safeguard its activities from cyber threats but is concerned that the Department remains indirectly vulnerable to cyber attack on critical pieces of civilian infrastructure not under the Department's protection. Because of the nature of their location and construction, U.S. military installations are often supported by the surrounding communities' infrastructure, including civilian power grids, public works, and telecommunications networks. Many of these utilities are poorly protected or completely unprotected from potential cyber attacks. Loss of service from these utilities could have significant implications on the Department's ability to assure mission critical capabilities.

Therefore, the committee directs the Secretary of Defense to conduct a study on the threat to the readiness of military installations from possible cyber attacks on civilian critical infrastructure, and brief the results of that study along with a plan to mitigate any risk associated with this vulnerability to the Senate Committee on Armed Services and the House Committee on Armed Services within 180 days after the date of enactment of this Act.

Economic Warfare

The committee is aware that the national security posture of the Nation is directly tied to the health and vitality of the economy. Periods of economic hardship have historically caused pressures on budgeting, execution, and planning for defense capabilities, and thus can slow or halt acquisition and modernization activities. Since U.S. military strength is underpinned by its technological superiority, the committee is aware of the direct dependency that military strength has on economic health.

The committee is concerned that our adversaries understand this dependency, and are developing means to attack our military strength by attacking our economy. The committee is aware that in public statements and documents, Al Qaeda has discussed "bleeding the Nation dry" through economic attacks, and has conducted a number of physical attacks internationally in order to cause economic damage. In addition, other nations have written about using economic warfare to complement or support military actions. Historically, even the United States has planned for and conducted economic warfare to subvert adversaries during World War II and the cold war.

The committee is aware that there is a 2009 report from the Irregular Warfare Support Program titled "Economic Warfare: Risks and Responses" offered plausible scenarios about how economic warfare might be used against the United

States. The committee is concerned that there does not appear to be any organization within the Department responsible for looking at the threats of economic warfare, or the impact economic attacks might have on military capabilities.

Therefore, the committee directs the Director of the Office of Net Assessment to conduct a study on economic warfare threats to the United States and deliver a report on the findings to the Senate Committee on Armed Services and the House Committee on Armed Services within 180 days after the date of enactment of this Act.

. Planning for Electromagnetic Pulse Events

The committee remains concerned with the continued vulnerability of the United States homeland to electromagnetic pulse (EMP) events, both man-made and naturally occurring. The 2008 report of the EMP Commission found that "EMP generated by a high altitude nuclear explosion is one of a small number of threats that can hold our society at risk of catastrophic consequences." The committee believes that the Secretary of Defense should ensure that the U.S. Military has the appropriate authorities, capabilities, procedures, protections, and force structure to defend against any threats posed by EMP generated by a high altitude nuclear or by a naturally occurring event. As well as response plans for dealing with the aftermath of an EMP event.

Therefore, the committee directs the Secretary of Defense to provide a report to the Senate Committee on Armed Services and the House Committee on Armed Services on efforts to prepare for and defend against, and remediate after an EMP event, whether natural or manmade. Within 120 days after the date of enactment of this Act the report should include the following:

(1) An assessment of any threats posed by a natural or manmade EMP event, including identifying of the foreign countries that may be developing weapons capable of producing high altitude EMP, the nature of the capabilities, and possible advances in the capabilities over the next 10 years;
(2) A description of any efforts by the Department of Defense since the 2008 EMP Commission Report was released to address the findings in (1);
(3) A description of the appropriate authorities, capabilities, procedures, protections, and force structure that the United States may require over the next 10 years to address the findings in (1);
(4) A description of Government contingency response plans to mitigate the consequences of or remediate after an EMP event, especially with regard to critical infrastructure;
(5) In the event that no Government contingency response plans exist, a description of what steps are being undertaken by the Department on an emergency basis to respond to an EMP event;
(6) A description of plans and guidance for military base commanders to be prepared to act on their own authority to provide support to or receive

support from local authorities, police, fire, and other emergency services, as well as plans and training with civil first responders in their locality to help restore critical infrastructures and assist the civilian population after a catastrophic EMP event and;

(7) An assessment of additional legal authorities or resources that may be needed to develop contingency response plans and capabilities to protect the American people and remediate critical infrastructures after an EMP event.

The Role of Military Information Support Operations

The committee is aware of the Secretary of Defense's directed name change from Psychological Operations to Military Information Support Operations (MISO). This committee is also aware of an ongoing implementation strategy that will institutionalize this change within the Department. While the committee understands the rationale for this change, the committee notes with concern that the Department did not consult the congressional defense committees in a timely fashion as the Psychological Operations activity and mission is codified in Section 167 and Section 2011 of title 10, United States Code.

The committee supports efforts by the Commander, U.S. Special Operations Command (USSOCOM) and the Assistant Secretary of Defense for Special Operations, Low Intensity Conflict and Interdependent Capabilities to support geographic combatant commander and chiefs of mission requirements through the deployment of Military Information Support Teams and Regional Military Information Support Teams. The committee is encouraged that the Assistant Secretary has recently established an Information Operations Directorate dedicated to information operations (IO) and MISO, and supports ongoing reviews to improve the force structure and readiness framework of the Active Component of MISO through the establishment of the MISO Command. The committee expects these changes to contribute to a more comprehensive information operations and strategic communication (IO/SC) strategy that will effectively utilize and incorporate MISO to inform and influence foreign audiences with cultural precision and enable geographic combatant commanders and chiefs of mission to counter enemy narratives and activities.

However, the committee is concerned about a growing operational, technical, and capability divide between the Active and Reserve Components of MISO forces which could limit options available to geographic combatant commanders and chiefs of mission as a tool to satisfy critical IO/SC requirements. The committee is further concerned about deficiencies in the reserve component of MISO and the resultant capabilities gap to provide support to the general purpose forces across the full spectrum of MISO. This capability divide between Active and Reserve components could fracture overall U.S. Government efforts and activities, and limit the ability to field a globally persistent and culturally aware MISO force that is capable of informing and influencing foreign audiences, contributing to strategic and tactical IO/SC requirements, and integrating with other information disciplines.

While the committee is encouraged that USSOCOM is shifting overseas contingency operations funds into base budget funds for Major Force Program (MFP) 11 funded MISO, it is concerned that a similar program shift is not taking place for the Reserve Component of MISO and therefore may potentially constitute a force structure, limited in capability, that is dependent on Overseas Contingency Operations funds.

Therefore, the committee directs the Assistant Secretary of Defense for Special Operations, Low Intensity Conflict and Interdependent Capabilities in coordination with the Commander, USSOCOM to provide a report to the congressional defense committees that outlines: a comprehensive MISO strategy to include the roles, missions, authorities, and capabilities of MISO Active and Reserve Components; current and future force structure requirements, operational limitations and constraints; and efforts to shift required Active and Reserve Component funding from overseas contingency operations to base funding to support future active and reserve force structure requirements. The report should also examine and include recommendations for the potential transfer of proponency of the MISO Reserve Component from USSOCOM to the Department of the Army, similar to the potential transfer of proponency responsibilities for U.S. Army Reserve Component Civil Affairs forces. The report should also include an analysis of the relationship among all IO/SC disciplines to determine if they are sufficient or could be improved through changes to authorities, processes, procedures, and synchronization mechanisms. The committee further directs the Assistant Secretary to submit the report to the congressional defense committees in unclassified format (with a classified annex as required) within 180 days after the date of enactment of this Act.