AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

109TH CONGRESS, 2d Session | HOUSE OF REPRESENTATIVES | REPT. 109–713, Part 1

DEPARTMENT OF HOMELAND SECURITY AUTHORIZATION ACT FOR FISCAL YEAR 2007

NOVEMBER 9, 2006.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. KING of New York, from the Committee on Homeland Security, submitted the following

R E P O R T

together with

MINORITY VIEWS

[To accompany H.R. 5814]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 5814) to authorize appropriations for the Department of Homeland Security, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
Purpose and Summary	67
Background and Need for Legislation	67
Hearings	68
Committee Consideration	71
Committee Votes	71
Committee Oversight Findings	87
Statement of General Performance Goals and Objectives	87
New Budget Authority, Entitlement Authority, and Tax Expenditures	87
Congressional Budget Office Estimate	87
Federal Mandates Statement	94
Compliance with House Resolution 1000	94
Advisory Committee Statement	94
Constitutional Authority Statement	95
Applicability to Legislative Branch	95
Section-by-Section Analysis of the Legislation	95
Changes in Existing Law Made by the Bill, as Reported	128
Minority Views	210

59–011

The amendment is as follows:
Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Department of Homeland Security Authorization Act for Fiscal Year 2007".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.

TITLE I—AUTHORIZATION OF APPROPRIATIONS

Sec. 101. Department of Homeland Security.

TITLE II—IMPROVING MANAGEMENT, INTEGRATION, AND OVERSIGHT

Subtitle A—Management Reform

Sec. 201. Abolishment of Under Secretary for Management.
Sec. 202. Providing direct line authority for chief operating officers.
Sec. 203. Emergency planning and response for individuals with disabilities.
Sec. 204. Government Accountability Office study on accessibility of emergency shelters.
Sec. 205. Homeland Security Education Program.

Subtitle B—Integration and Organizational Improvements

Sec. 221. Establishment of Directorate for Policy, Planning, and International Affairs.
Sec. 222. Consolidation of the efforts of the Center for Domestic Preparedness and the Noble Training Center.
Sec. 223. Government Accountability Office study of integration and adequacy of training programs related to asylum at ports of entry.

Subtitle C—Strengthening Oversight

Sec. 231. Congressional notification requirement.
Sec. 232. Authorization Liaison Officer.
Sec. 233. Required budget line item for Office of Counternarcotics Enforcement.
Sec. 234. Secure border initiative financial accountability.

TITLE III—PROCUREMENT REFORM

Sec. 301. Homeland security procurement training.
Sec. 302. Additional requirements to review past performance of contractors.
Sec. 303. Streamlining of SAFETY Act and procurement processes.
Sec. 304. Comptroller General report on Department of Homeland Security Contracting.
Sec. 305. Contracting requirements.
Sec. 306. Certification requirements for offerors for Department of Homeland Security contracts.
Sec. 307. Contracts for assistance activities relating to acts of terrorism, natural disasters, and other emergencies.
Sec. 308. Emergency contracting support annex.
Sec. 309. Increased Inspector General oversight.
Sec. 310. Purchase cards.

TITLE IV—PERSONNEL AUTHORITIES

Subtitle A—Workforce Enhancements

Sec. 401. Cost-effective training for border patrol agents.
Sec. 402. Continuation of Federal law enforcement training center authority to appoint and maintain a cadre of Federal annuitants to support training.
Sec. 403. Canine detection team coordination and certification.
Sec. 404. Authority for Customs and Border Protection to appoint and maintain a cadre of Federal annuitants.
Sec. 405. Strengthening border patrol recruitment and retention.
Sec. 406. Customs and Border Protection Officer Pay Equity.

Subtitle B—Improving Security Clearance Process

Sec. 411. Increased security screening of Homeland Security Officials.
Sec. 412. Authorities of Chief Security Officer.

TITLE V—INTELLIGENCE AND INFORMATION SHARING

Sec. 501. Departmental reorganization.
Sec. 502. Intelligence components of Department of Homeland Security.
Sec. 503. Homeland Security Advisory System.
Sec. 504. Homeland security information sharing.
Sec. 505. State, Local, Tribal, and Regional Information Fusion Center Initiative.
Sec. 506. Homeland Security Information Sharing Fellows Program.
Sec. 507. Full and efficient use of open-source intelligence.
Sec. 508. Strengthening the capabilities of the Human Smuggling and Trafficking Center.

TITLE VI—PREVENTION OF NUCLEAR AND BIOLOGICAL TERRORISM

Sec. 601. Establishment of Office of Domestic Nuclear Detection.
Sec. 602. Chief Medical Officer.
Sec. 603. National Biosurveillance Integration System.
Sec. 604. Material threats.
Sec. 605. Study on national biodefense training.
Sec. 606. Homeland Security Science and Technology Advisory Committee.

TITLE VII—HOMELAND SECURITY INFRASTRUCTURE PROTECTION AND CYBERSECURITY ENHANCEMENT

Sec. 701. Infrastructure Protection and Cybersecurity.

Sec. 702. Critical infrastructure study.
Sec. 703. Cybersecurity Training Program and Equipment.
Sec. 704. National Asset Database.

TITLE VIII—GRANTS ADMINISTRATION

Sec. 801. Faster and smarter funding for first responders.
Sec. 802. Authorization of appropriations.
Sec. 803. Metropolitan Medical Response System.

TITLE IX—TRANSPORTATION SECURITY

Subtitle A—Rail and Public Transportation Security

Sec. 901. Transportation security.
Sec. 902. Rulemaking requirements.
Sec. 903. Rail and public transportation security training program.
Sec. 904. Interagency cooperation.
Sec. 905. Rail and public transportation security grant program.
Sec. 906. Rail and public transportation security exercise program.
Sec. 907. Authorization of Appropriations.

Subtitle B—Transportation Security Operations Enhancements

Sec. 911. Aviation security funding.
Sec. 912. Research and development of transportation security technology.
Sec. 913. Enforcement authority in nonaviation transportation.
Sec. 914. Liability for security screening inspections.
Sec. 915. Temporary private screener assistance.
Sec. 916. Recurrent training to operate certain aircraft.
Sec. 917. Annual report on unclaimed money recovered.

Subtitle C—Passenger Screening

Sec. 921. Passenger identification documents.
Sec. 922. International passenger prescreening.
Sec. 923. International cooperative efforts.
Sec. 924. Computer assisted passenger prescreening system.
Sec. 925. Federal flight deck officers.
Sec. 926. Enhanced perimeter security and access control through comprehensive screening of airport workers.
Sec. 927. Prohibited items.
Sec. 928. Secured areas of airports.
Sec. 929. Repair Stations.

Subtitle D—Technical Amendments

Sec. 931. Reporting requirements repealed.
Sec. 932. Consolidation of reports.
Sec. 933. Aircraft charter customer and lessee prescreening.

TITLE X—MISCELLANEOUS PROVISIONS

Sec. 1001. Protection of Department of Homeland Security name, initials, insignia, and seal.
Sec. 1002. Authorized use of surplus military vehicles.
Sec. 1003. Encouraging use of computerized training aids.
Sec. 1004. Emergency notification system study deadline.
Sec. 1005. Report on fraud prevention exercises.
Sec. 1006. Limitation on reimbursements relating to certain detailees.

TITLE I—AUTHORIZATION OF APPROPRIATIONS

SEC. 101. DEPARTMENT OF HOMELAND SECURITY.

There is authorized to be appropriated to the Secretary of Homeland Security for the necessary expenses of the Department of Homeland Security for fiscal year 2007, $34,698,270,000.

TITLE II—IMPROVING MANAGEMENT, INTEGRATION, AND OVERSIGHT

Subtitle A—Management Reform

SEC. 201. ABOLISHMENT OF UNDER SECRETARY FOR MANAGEMENT.

(a) ABOLISHMENT.—Section 701 and section 702 of the Homeland Security Act of 2002 (6 U.S.C. 341 and 342) are amended by striking "Under Secretary for Management" each place such term appears and inserting "Deputy Secretary" .

(b) CONFORMING AMENDMENT.—

(1) Section 103(a) of the Homeland Security Act of 2002 (6 U.S.C. 113(a)) is amended by striking paragraph (7) and redesignating paragraphs (8) through (10) as paragraphs (7) through (9), respectively.

(2) The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the item relating to section 701 and inserting the following:

"Sec. 701. Deputy Secretary.".

(3) The heading for section 701 of the Homeland Security Act of 2002 (6 U.S.C. 341) is amended to read as follows:

"SEC. 701. DEPUTY SECRETARY.".

SEC. 202. PROVIDING DIRECT LINE AUTHORITY FOR CHIEF OPERATING OFFICERS.

(a) IN GENERAL.—The Department's Chief Operating Officers shall include the following:

(1) the Chief Financial Officer;
(2) the Chief Procurement Officer;
(3) the Chief Information Officer;
(4) the Chief Human Resources Officer;
(5) the Chief Administrative Officer; and
(6) the Chief Security Officer.

(b) DELEGATION.—The Secretary shall delegate to the Chief Operating Officers direct authority over their respective counterparts in component agencies to ensure that the component agencies adhere to the laws, rules, regulations, and departmental policies for which the Chief Operating Officers are responsible for implementing. In coordination with the head of the relevant component agency, such authorities shall include, with respect to the Officer's counterparts within component agencies of the Department, the following:

(1) the ability to direct the activities of personnel;
(2) the ability to direct planning, operations, and training; and
(3) the ability to direct the budget and other financial resources.

(c) COORDINATION WITH HEADS OF COMPONENT AGENCIES.—The Chief Operating Officers in component agencies shall coordinate with the heads of their respective agencies while fulfilling their responsibilities under subsection (b) to report directly to the Chief Operating Officers referred to in subsection (a).

SEC. 203. EMERGENCY PLANNING AND RESPONSE FOR INDIVIDUALS WITH DISABILITIES.

(a) OFFICER FOR CIVIL RIGHTS AND CIVIL LIBERTIES AS COORDINATOR FOR THE SECRETARY.—Section 705(a) of the Homeland Security Act of 2002 (6 U.S.C. 345(a)) is amended by striking "and" after the semicolon at the end of paragraph (5), by striking the period at the end of paragraph (6) and inserting "; and", and by adding at the end the following:

"(7) serve as the Secretary's coordinator for issues relating to individuals with disabilities and mitigation, preparedness, response, and recovery, by assisting the Secretary and directorates and offices of the Department to develop, implement, and periodically review relevant policies and procedures.".

(b) COORDINATOR FOR DIRECTOR OF FEMA.—Section 507 of the Homeland Security Act of 2002 (6 U.S.C. 317) is amended by adding at the end the following:

"(c) COORDINATOR FOR ISSUES RELATING TO INDIVIDUALS WITH DISABILITIES.—The Director of the Federal Emergency Management Agency shall appoint an individual to serve as the Director's coordinator for issues relating to individuals with disabilities. Such individual shall report to the Director and to the Officer for Civil Rights and Civil Liberties.".

(c) COORDINATOR FOR UNDER SECRETARY FOR PREPAREDNESS.—Section 502 of the Homeland Security Act of 2002 (6 U.S.C. 312) is amended by inserting "(a) IN GENERAL.—" before "The Secretary", and by adding at the end the following:

"(b) COORDINATOR FOR ISSUES RELATING TO INDIVIDUALS WITH DISABILITIES.—The Under Secretary for Preparedness shall appoint a coordinator for issues relating to individuals with disabilities. Such individual shall report to the Under Secretary and to the Officer for Civil Rights and Civil Liberties.".

SEC. 204. GOVERNMENT ACCOUNTABILITY OFFICE STUDY ON ACCESSIBILITY OF EMERGENCY SHELTERS.

(a) IN GENERAL.—The Comptroller General of the United States shall conduct a national study regarding whether, and, if so, to what extent, emergency shelters for use in response to a major disaster, as that term is defined in section 102(2) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122(2)), are accessible to, and usable by, individuals with disabilities.

(b) REPORT.—Not later than 12 months after the date of enactment of this Act, the Comptroller General shall submit to Congress a report summarizing the results of the study under subsection (a).

SEC. 205. HOMELAND SECURITY EDUCATION PROGRAM.

(a) ESTABLISHMENT.—The Secretary, acting through the Department official with primary responsibility for grants and training, shall establish a graduate-level Homeland Security Education Program in the National Capital Region to provide educational opportunities to senior Federal officials and selected State and local officials with homeland security and emergency management responsibilities. The Secretary shall give particular consideration to including in the Program minority serving institutions.

(b) LEVERAGING OF EXISTING RESOURCES.—To maximize efficiency and effectiveness in carrying out the Program, the Secretary shall use existing Department-reviewed Master's Degree curricula in homeland security, including curricula pending accreditation, together with associated learning materials, quality assessment tools, digital libraries, exercise systems and other curriculum components already being delivered by Federal, State, and private universities and educational facilities, including the National Domestic Preparedness Consortium, the National Fire Academy, and the Emergency Management Institute.

(c) STUDENT ENROLLMENT.—

(1) SOURCES.—The student body of the Program shall include officials from Federal, State, tribal, and local governments, and from other sources designated by the Secretary.

(2) ENROLLMENT PRIORITIES AND SELECTION CRITERIA.—The Secretary shall establish policies governing student enrollment priorities and selection criteria that are consistent with the mission of the Program.

(3) DIVERSITY.—The Secretary shall take reasonable steps to ensure that the student body represents racial, gender, and ethnic diversity.

(d) SERVICE COMMITMENT.—

(1) IN GENERAL.—Before any employee selected for the Program may be assigned to such education, the employee shall agree in writing to—

(A) continue in the service of the agency sponsoring the employee during the two-year period beginning on the date on which the employee completes the program, unless the employee is involuntarily separated from the service of that agency for reasons other than reduction in force; and

(B) pay to the Government the amount of the additional expenses incurred by the Government in connection with the employee's education if the employee is voluntarily separated from the service to the agency before the end of the period described in subparagraph (A).

(2) PAYMENT OF EXPENSES.—

(A) EXEMPTION.—An employee who leaves the service of the sponsoring agency to enter into the service of another agency in any branch of the Government shall not be required to make a payment under paragraph (1)(B), unless the head of the agency that sponsored the education of the employee notifies the employee before the date on which the employee enters the service of the other agency that payment is required under that paragraph.

(B) AMOUNT OF PAYMENT.—If an employee is required to make a payment under paragraph (1)(B), the agency that sponsored the education of the employee shall determine the amount of the payment, except that such amount may not exceed the pro rata share of the expenses incurred for the time remaining in the two-year period.

(3) RECOVERY OF PAYMENT.—If an employee who is required to make a payment under this subsection does not make the payment, a sum equal to the amount of the expenses incurred by the Government for the education of that employee is recoverable by the Government from the employee or his estate by—

(A) setoff against accrued pay, compensation, amount of retirement credit, or other amount due to the employee from the Government; or

(B) such other method as is provided by law for the recovery of amounts owing to the Government.

Subtitle B—Integration and Organizational Improvements

SEC. 221. ESTABLISHMENT OF DIRECTORATE FOR POLICY, PLANNING, AND INTERNATIONAL AFFAIRS.

(a) ESTABLISHMENT.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) by redesignating title VI as subtitle B of title XVIII, and moving such title so as to appear after subtitle A of title XVIII, as added by section 403;

(2) by striking the heading of such title and inserting the following:

"Subtitle B—Treatment of Certain Charitable Trusts".

(3) by redesignating section 601 as section 1811; and
(4) by inserting after title V the following new title:

"TITLE VI—POLICY, PLANNING, AND INTERNATIONAL AFFAIRS

"SEC. 601. DIRECTORATE FOR POLICY, PLANNING, AND INTERNATIONAL AFFAIRS.

"(a) ESTABLISHMENT.—There is in the Department a Directorate for Policy, Planning, and International Affairs.

"(b) UNDER SECRETARY FOR POLICY.—

"(1) IN GENERAL.—The head of the Directorate is the Under Secretary for Policy, who shall be appointed by the President.

"(2) QUALIFICATIONS.—No individual shall be appointed Under Secretary for Policy under paragraph (1) unless the individual has, by education and experience, demonstrated knowledge, ability, and skill in the fields of policy and strategic planning.

"(c) RESPONSIBILITIES OF UNDER SECRETARY.—

"(1) POLICY RESPONSIBILITIES.—Subject to the direction and control of the Secretary, the policy responsibilities of the Under Secretary for Policy shall be as follows:

"(A) To serve as the principal policy advisor to the Secretary.

"(B) To provide overall direction and supervision of policy development for the programs, offices, and activities of the Department.

"(C) To establish and implement a formal policymaking process for the Department.

"(D) To analyze, evaluate, and review the completed, ongoing, and proposed programs of the Department to ensure they are compatible with the statutory and regulatory responsibilities of the Department and with the Secretary's priorities, strategic plans, and policies.

"(E) To ensure that the budget of the Department (including the development of future year budgets and interaction with the Office of Management and Budget and with Congress) is compatible with the statutory and regulatory responsibilities of the Department and with the Secretary's priorities, strategic plans, and policies.

"(F) To represent the Department in any development of policy that requires the Department to consult with another Federal agency, the Office of the President, a foreign government, or any other governmental or private sector entity.

"(G) To supervise and oversee policy development undertaken by the component agencies and offices of the Department.

"(H) To provide for the coordination and maintenance of the trade and customs revenue functions of the Department.

"(2) STRATEGIC PLANNING RESPONSIBILITIES.—Subject to the direction and control of the Secretary, the strategic planning responsibilities of the Under Secretary for Policy shall be as follows:

"(A) To conduct long-range, strategic planning for the Department.

"(B) To prepare national and Department strategies, as appropriate.

"(C) To conduct net assessments of issues facing the Department.

"(3) INTERNATIONAL RESPONSIBILITIES.—Subject to the direction and control of the Secretary, the international responsibilities of the Under Secretary for Policy shall be as follows:

"(A) To promote the exchange of information and the sharing of best practices and technology relating to homeland security with nations friendly to the United States, including—

"(i) the exchange of information on research and development on homeland security technologies in coordination with the Under Secretary for Science and Technology;

"(ii) joint training exercises of first responders in coordination with the Department official with primary responsibility for grants and training; and

"(iii) exchanging expertise and information on terrorism prevention, response, and crisis management in coordination with the Director of the Federal Emergency Management Agency.

"(B) To identify any homeland security-related area in which the United States and other nations and appropriate international organizations could collaborate to improve capabilities and to encourage the exchange of information or sharing of best practices and technology relating to that area.

"(C) To plan and participate in international conferences, exchange programs (including the exchange of scientists, engineers, and other experts), and other training activities with friendly nations in coordination with the Under Secretary for Science and Technology.

"(D) To manage international activities within the Department in coordination with other Federal officials with responsibility for counterterrorism matters.

"(E) To oversee the activities of Department personnel operating in other countries or traveling to other countries.

"(F) To represent the Department in international negotiations and working groups.

"(4) PRIVATE SECTOR.—

"(A) To create and foster strategic communications with the private sector to enhance the primary mission of the Department to protect the United States.

"(B) To advise the Secretary on the impact on the private sector of the policies, regulations, processes, and actions of the Department.

"(C) To create and manage private sector advisory councils composed of representatives of industries and associations designated by the Secretary—

"(i) to advise the Secretary on private sector products, applications, and solutions as they relate to homeland security challenges; and

"(ii) to advise the Secretary on homeland security policies, regulations, processes, and actions that affect the participating industries and associations.

"(D) To promote existing public-private partnerships and develop new public-private partnerships to provide for collaboration and mutual support to address homeland security challenges.

"(E) To identify private sector resources and capabilities that could be effective in supplementing functions of the Department and State and local governments to prevent or respond to acts of terrorism.

"(F) To coordinate among the Department's operating entities and with the Assistant Secretary for Trade Development of the Department of Commerce on issues related to the travel and tourism industries.

"(5) TRADE AND CUSTOMS REVENUE FUNCTIONS.—The Under Secretary for Policy shall—

"(A) ensure that the trade and customs revenue functions of the Department are coordinated within the Department and with other Federal departments and agencies, and that the impact on legitimate trade is taken into account in any action impacting these functions; and

"(B) monitor and report to Congress on the Department's mandate to ensure that the trade and customs revenue functions of the Department are not diminished, including how spending, operations, and personnel related to these functions have kept pace with the level of trade entering the United States.

"SEC. 602. OFFICE OF INTERNATIONAL AFFAIRS.

"(a) ESTABLISHMENT.—There is established within the Directorate of Policy, Planning, and International Affairs an Office of International Affairs. The Office shall be headed by an Assistant Secretary, who shall be appointed by the Secretary.

"(b) DUTIES OF THE ASSISTANT SECRETARY.—The Assistant Secretary for International Affairs, in coordination with the Under Secretary for Science and Technology, the Director of the Federal Emergency Management Agency, the Department official with primary responsibility for grants and training, and other officials of the Department, as appropriate, shall have the following duties:

"(1) To promote information and education exchange with nations friendly to the United States in order to promote sharing of best practices and technologies relating to homeland security. Such exchange shall include the following:

"(A) Exchange of information on research and development on homeland security technologies.

"(B) Joint training exercises of first responders.

"(C) Exchange of expertise on terrorism prevention, response, and crisis management.

"(2) To identify areas for homeland security information and training exchange where the United States has a demonstrated weakness and another friendly nation or nations have a demonstrated expertise.

"(3) To plan and undertake international conferences, exchange programs, and training activities.

"(4) To manage international activities within the Department in coordination with other Federal officials with responsibility for counter-terrorism matters.

"SEC. 603. OTHER OFFICES AND OFFICIALS.

"(a) IN GENERAL.—The Under Secretary for Policy shall establish the following offices in the Directorate for Policy, Planning, and International Affairs:

"(1) The Office of Policy, which shall be administered by an Assistant Secretary for Policy.

"(2) The Office of Strategic Plans, which shall be administered by an Assistant Secretary for Strategic Plans and which shall include—

"(A) a Secure Border Initiative Program Office; and

"(B) a Screening Coordination and Operations Office.

"(3) The Office of the Private Sector, which shall be administered by an Assistant Secretary for the Private Sector.

"(4) The Victim Assistance Officer.

"(5) The Tribal Security Officer.

"(6) Such other offices as considered necessary by the Under Secretary for Policy.

"(b) DIRECTOR OF CARGO SECURITY POLICY.—

"(1) IN GENERAL.—There shall be in the Directorate for Policy, Planning, and International Affairs a Director of Cargo Security Policy (hereinafter in this subsection referred to as the 'Director'), who shall be subject to the direction and control of the Under Secretary for Policy.

"(2) RESPONSIBILITIES.—The Director shall—

"(A) advise the Assistant Secretary for Policy regarding all aspects of Department programs relating to cargo security;

"(B) develop Department-wide policies regarding cargo security; and

"(C) coordinate the cargo security policies and programs of the Department with other Federal departments and agencies, including by working with officials of the Department of Energy and the Department of State, as appropriate, in negotiating international agreements relating to cargo security.

"(c) DIRECTOR OF TRADE POLICY.—

"(1) IN GENERAL.—There shall be in the Directorate for Policy, Planning, and International Affairs a Director of Trade Policy (hereinafter in this subsection referred to as the 'Director'), who shall be subject to the direction and control of the Under Secretary for Policy.

"(2) RESPONSIBILITIES.—The Director shall—

"(A) advise the Assistant Secretary for Policy regarding all aspects of Department programs relating to the trade and customs revenue functions of the Department;

"(B) develop Department-wide policies regarding trade and customs revenue functions and trade facilitation; and

"(C) coordinate the trade and customs revenue-related programs of the Department with other Federal departments and agencies.

"SEC. 604. CONSULTATION ON TRADE AND CUSTOMS REVENUE FUNCTIONS.

"(a) IN GENERAL.—The Secretary and the Under Secretary for Policy shall consult with representatives of the business community involved in international trade, including seeking the advice and recommendations of the Commercial Operations Advisory Committee (COAC), on Department policies and actions that have a significant impact on international trade and customs revenue functions.

"(b) COAC CONSULTATION AND NOTIFICATION.—

"(1) IN GENERAL.—Subject to paragraph (2), the Secretary shall seek the advice and recommendations of COAC on any proposed Department policies, initiatives, actions, or organizational reforms that will have a major impact on trade and customs revenue functions not later than 45 days prior to the finalization of the policies, initiatives, actions, or organizational reforms.

"(2) EXCEPTION.—If the Secretary determines that it is important to the national security interest of the United States to finalize any proposed Department policies, initiatives, actions, or organizational reforms prior to the provision of advice and recommendations described in paragraph (1), the Secretary shall—

"(A) seek the advice and recommendations of COAC on the policies, initiatives, actions, or organizational reforms not later than 30 days after the

date on which the policies, initiatives, actions, or organizational reforms are finalized; and

"(B) to the extent appropriate, modify the policies, initiatives, actions, or organizational reforms based upon the advice and recommendations of COAC.

"(c) CONGRESSIONAL CONSULTATION AND NOTIFICATION.—

"(1) IN GENERAL.—Subject to paragraph (2), the Secretary shall consult with and provide any recommendations of COAC received under subsection (b) to the appropriate congressional committees not later than 30 days prior to the finalization of any Department policies, initiatives, actions or organizational reforms that will have a major impact on trade and customs revenue functions.

"(2) EXCEPTION.—If the Secretary determines that it is important to the national security interest of the United States to finalize any Department policies, initiatives, actions, or organizational reforms prior to the consultation described in paragraph (1), the Secretary shall—

"(A) consult with and provide any recommendations of COAC received under subsection (b) to the appropriate congressional committees not later than 30 days after the date on which the policies, initiative, actions, or organizational reforms are finalized; and

"(B) to the extent appropriate, modify the policies, initiatives, actions, or organizational reforms based upon the consultations with the appropriate congressional committees.".

(b) CONFORMING AMENDMENT.—Section 879 of the Homeland Security Act of 2002 (6 U.S.C. 459) is repealed.

(c) CLERICAL AMENDMENTS.—The table of contents in section 1(b) of such Act is amended—

(1) by striking the item relating to section 879;

(2) by striking the items relating to title VI and inserting the following:

"TITLE VI—POLICY, PLANNING, AND INTERNATIONAL AFFAIRS

"Sec. 601. Directorate for Policy, Planning, and International Affairs.
"Sec. 602. Office of International Affairs.
"Sec. 603. Other offices and officials.
"Sec. 604. Consultation on trade and customs revenue functions."; and

(3) by inserting after the items relating to subtitle A of title XVIII, as added by section 403, the following:

"Subtitle B—Treatment of Certain Charitable Trusts

"Sec. 1811.Treatment of charitable trusts for members of the armed forces of the United States and other governmental organizations.".

SEC. 222. CONSOLIDATION OF THE EFFORTS OF THE CENTER FOR DOMESTIC PREPAREDNESS AND THE NOBLE TRAINING CENTER.

(a) TRANSFER.—The Noble Training Center is transferred to the Center for Domestic Preparedness. The Center for Domestic Preparedness shall integrate the Noble Training Center into the program structure of the Center for Domestic Preparedness.

(b) EXECUTIVE SERVICE DESIGNATION FOR DIRECTOR OF CENTER FOR DOMESTIC PREPAREDNESS.—The Director of the Center for Domestic Preparedness of the Department of Homeland Security shall be a career appointee in the Senior Executive Service.

(c) CENTER FOR DOMESTIC PREPAREDNESS FACILITY MANAGEMENT.—The Director of the Center for Domestic Preparedness is authorized to obtain the transfer of the United States Army In-Processing Center (commonly referred to as the 500 Area) and portions of the former Noncommissioned Officer Housing Dormitories (commonly referred to as the 900 Area) at the former Fort McClellan, Alabama, for use by the Center for Domestic Preparedness.

SEC. 223. GOVERNMENT ACCOUNTABILITY OFFICE STUDY OF INTEGRATION AND ADEQUACY OF TRAINING PROGRAMS RELATED TO ASYLUM AT PORTS OF ENTRY.

(a) IN GENERAL.—The Comptroller General shall conduct a study of the integration and adequacy of training for Department of Homeland Security personnel who interdict, interview, and process asylum seekers ports of entry, including at airports, in the United States.

(b) CONTENTS OF STUDY.—The study shall include—

(1) an assessment of whether such training provides such personnel with adequate and clear guidance on the standards for handling asylum seekers;

(2) an assessment of whether such personnel coordinate appropriately to ensure that relevant United States laws are fully enforced; and

(3) recommendations, as appropriate, for steps that the Secretary of Homeland Security should take to provide better integration and adequacy of such

training to such personnel in order to better secure the borders of the United States while ensuring that asylum seekers are properly processed and their claims are fully evaluated.

(c) REPORT.—Not later than 12 months after the date of the enactment of this Act, the Comptroller General shall submit a report summarizing the results of the study to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

Subtitle C—Strengthening Oversight

SEC. 231. CONGRESSIONAL NOTIFICATION REQUIREMENT.

(a) IN GENERAL.—Title I of the Homeland Security Act of 2002 (6 U.S.C. 111 et seq.) is amended by adding at the end the following:

"SEC. 104. CONGRESSIONAL NOTIFICATION.

"(a) IN GENERAL.—The Secretary shall actively consult with the congressional homeland security committees, and shall keep such committees fully and currently informed with respect to all activities and responsibilities within the jurisdictions of these committees.

"(b) RELATIONSHIP TO OTHER LAW.—Nothing in this section affects the requirements of section 872. The requirements of this section supplement, and do not replace, the requirements of that section.

"(c) INSPECTOR GENERAL.—The Inspector General of the Department shall be responsible, independently of the responsibility of the Secretary under subsection (a), for keeping the congressional homeland security committees fully and currently informed of the Department's activities, including informing the congressional homeland security committees of major audits, investigations, or other activities of the Inspector General by no later than 72 hours prior to the release of, or at any time upon the request by such a committee for, the findings of major audits, investigations, or other activities. Additionally, the Inspector General shall provide to such a committee a written notification and summary of the contents of its semiannual and annual reports by no later than 72 hours prior to the release of such reports.

"(d) CLASSIFIED NOTIFICATION.—The Secretary may submit any information required by this section in classified form if the information is classified pursuant to applicable national security standards.

"(e) SAVINGS CLAUSE.—This section shall not be construed to limit or otherwise affect the congressional notification requirements of title V of the National Security Act of 1947 (50 U.S.C. 413 et seq.), insofar as they apply to the Department.

"(f) DEFINITION.—As used in this section, the term 'congressional homeland security committees' means the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate.".

(b) CONFORMING AMENDMENT.—The table of contents in Section 1(a) of such Act is amended by inserting after the item relating to section 103 the following:

"Sec. 104. Congressional notification.".

(c) COAST GUARD MISSION REVIEW REPORT.—Section 888(f)(2) of the Homeland Security Act of 2002 (6 U.S.C. 468(f)(2)) is amended—

(1) by redesignating subparagraphs (B) through (E) as subparagraphs (C) through (F), respectively; and

(2) by striking subparagraph (A) and inserting the following:

"(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

"(B) the Committee on Homeland Security of the House of Representatives;".

SEC. 232. AUTHORIZATION LIAISON OFFICER.

Section 702 of the Homeland Security Act of 2002 (6 U.S.C. 342) is amended by adding at the end the following:

"(d) AUTHORIZATION LIAISON OFFICER.—

"(1) IN GENERAL.—The Chief Financial Officer shall establish the position of Authorization Liaison Officer to provide timely budget and other financial information to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate. The Authorization Liaison Officer shall report directly to the Chief Financial Officer.

"(2) SUBMISSION OF REPORTS TO CONGRESS.—The Authorization Liaison Officer shall coordinate with the Appropriations Liaison Officer within the Office

of the Chief Financial Officer to ensure, to the greatest extent possible, that all reports prepared for the Committees on Appropriations of the House of Representatives and the Senate are submitted concurrently to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.".

SEC. 233. REQUIRED BUDGET LINE ITEM FOR OFFICE OF COUNTERNARCOTICS ENFORCEMENT.

Section 1105(a) of title 31, United States Code, is amended—

(1) by redesignating the second paragraph (33) as paragraph (35); and

(2) in paragraph (35), as so redesignated, in subparagraph (A)—

(A) by striking "and" after the semicolon at the end of clause (ii);

(B) by striking the period at the end of clause (iii) and inserting "; and"; and

(C) by adding at the end the following:

"(iv) a separate line item for each such fiscal year for expenditures by the Office of Counternarcotics Enforcement of the Department of Homeland Security.".

SEC. 234. SECURE BORDER INITIATIVE FINANCIAL ACCOUNTABILITY.

(a) IN GENERAL.—The Inspector General of the Department of Homeland Security shall review each contract action related to the Department's Secure Border Initiative having a value greater than $20,000,000, to determine whether each such action fully complies with applicable cost requirements, performance objectives, program milestones, inclusion of small, minority, and women-owned business, and timelines. The Inspector General shall complete a review under this subsection with respect to a contract action—

(1) not later than 60 days after the date of the initiation of the action; and

(2) upon the conclusion of the performance of the contract.

(b) REPORT BY INSPECTOR GENERAL.—Upon completion of each review described in subsection (a), the Inspector General shall submit to the Secretary of Homeland Security a report containing the findings of the review, including findings regarding any cost overruns, significant delays in contract execution, lack of rigorous departmental contract management, insufficient departmental financial oversight, bundling that limits the ability of small business to compete, or other high risk business practices.

(c) REPORT BY SECRETARY.—Not later than 30 days after the receipt of each report required under subsection (b), the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the findings of the report by the Inspector General and the steps the Secretary has taken, or plans to take, to address the problems identified in such report.

(d) AUTHORIZATION OF APPROPRIATIONS.—In addition to amounts that are otherwise authorized to be appropriated to the Office of the Inspector General, an additional amount equal to at least five percent for fiscal year 2007, at least six percent for fiscal year 2008, and at least seven percent for fiscal year 2009 of the overall budget of the Office for each such fiscal year is authorized to be appropriated to the Office to enable the Office to carry out this section.

(e) ACTION BY INSPECTOR GENERAL.—In the event the Inspector General becomes aware of any improper conduct or wrongdoing in accordance with the contract review required under subsection (a), the Inspector General shall, as expeditiously as practicable, refer information related to such improper conduct or wrongdoing to the Secretary of Homeland Security or other appropriate official in the Department of Homeland Security for purposes of evaluating whether to suspend or debar the contractor.

TITLE III—PROCUREMENT REFORM

SEC. 301. HOMELAND SECURITY PROCUREMENT TRAINING.

(a) IN GENERAL.—Subtitle H of title VIII of the Homeland Security Act of 2002 is amended by adding at the end the following new section:

"SEC. 890A. HOMELAND SECURITY PROCUREMENT TRAINING.

"(a) ESTABLISHMENT.—The Chief Procurement Officer shall provide homeland security procurement training to acquisition employees.

"(b) RESPONSIBILITIES OF CHIEF PROCUREMENT OFFICER.—The Chief Procurement Officer shall carry out the following responsibilities:

"(1) Establish objectives to achieve the efficient and effective use of available acquisition resources by coordinating the acquisition education and training pro-

grams of the Department and tailoring them to support the careers of acquisition employees.

"(2) Develop, in consultation with the Council on Procurement Training established under subsection (d), the curriculum of the homeland security procurement training to be provided.

"(3) Establish, in consultation with the Council on Procurement Training, training standards, requirements, and courses to be required for acquisition employees.

"(4) Establish an appropriate centralized mechanism to control the allocation of resources for conducting such required courses and other training and education.

"(5) Select course providers and certify courses to ensure that the procurement training curriculum supports a coherent framework for the educational development of acquisition employees, including the provision of basic, intermediate, and advanced courses.

"(6) Publish an annual catalog that includes a list of the acquisition education and training courses.

"(7) Develop a system of maintaining records of student enrollment, and other data related to students and courses conducted pursuant to this section.

"(c) PROVISION OF INSTRUCTION.—The Chief Procurement Officer shall provide procurement training to acquisition employees of any office under subsection (d)(3). The appropriate member of the Council on Procurement Training may direct such an employee to receive procurement training.

"(d) COUNCIL ON PROCUREMENT TRAINING.—

"(1) ESTABLISHMENT.—The Secretary shall establish a Council on Procurement Training to advise and make policy and curriculum recommendations to the Chief Procurement Officer.

"(2) CHAIR OF COUNCIL.—The chair of the Council on Procurement Training shall be the Deputy Chief Procurement Officer.

"(3) MEMBERS.—The members of the Council on Procurement Training are the chief procurement officers of each of the following:

"(A) United States Customs and Border Protection.

"(B) The Transportation Security Administration.

"(C) The Office of Procurement Operations.

"(D) The Bureau of Immigration and Customs Enforcement.

"(E) The Federal Emergency Management Agency.

"(F) The Coast Guard.

"(G) The Federal Law Enforcement Training Center.

"(H) The United States Secret Service.

"(I) Such other entity as the Secretary determines is appropriate.

"(e) ACQUISITION EMPLOYEE DEFINED.—For purposes of this section, the term 'acquisition employee' means an employee serving under a career or career-conditional appointment in the competitive service or appointment of equivalent tenure in the excepted service of the Federal Government, at least 50 percent of whose assigned duties include acquisitions, procurement-related program management, or procurement-related oversight functions.

"(f) REPORT REQUIRED.—Not later than March 1 of each year, the Chief Procurement Officer shall submit to the Secretary a report on the procurement training provided under this section, which shall include information about student enrollment, students who enroll but do not attend courses, graduates, certifications, and other relevant information.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding at the end of the items relating to such subtitle the following:

"Sec. 890A. Homeland security procurement training.".

SEC. 302. ADDITIONAL REQUIREMENTS TO REVIEW PAST PERFORMANCE OF CONTRACTORS.

(a) CONSIDERATION OF CONTRACTOR PAST PERFORMANCE.—In awarding a contract to a contractor, the Secretary of Homeland Security shall consider the past performance of that contractor based on the review conducted under subsection (b).

(b) REVIEW REQUIRED.—Before awarding a contract to any contractor, including a contract to be awarded to a contractor that has previously provided or currently provides goods or services to the Department of Homeland Security, the Secretary of Homeland Security, acting through the appropriate contracting officer or officers of the Department, shall require the contractor to submit information regarding the contractor's past and current performance of Federal, State, and local government and private sector contracts.

(c) CONTACT OF RELEVANT OFFICIALS.—As part of any review of a contractor's past performance conducted under subsection (b), the Secretary, acting through an appropriate contracting officer of the Department, shall contact the relevant official who

administered or oversaw any contract performed by that contractor during the five-year period preceding the date on which the review begins.

SEC. 303. STREAMLINING OF SAFETY ACT AND PROCUREMENT PROCESSES.

(a) PERSONNEL.—The Secretary of Homeland Security shall ensure that, in addition to any scientific evaluation completed prior to the designation or certification of qualified anti-terrorism technologies under the SAFETY Act (6 U.S.C. 441), a sufficient number of full-time equivalent personnel, who are properly trained and qualified to apply legal, economic, and risk analyses, are involved in the review and prioritization of anti-terrorism technologies for the purpose of determining whether such technologies may be designated by the Secretary as qualified anti-terrorism technologies under section 862(b) of the SAFETY Act (6 U.S.C. 441(b)) or certified by the Secretary under section 863(d) of such Act (6 U.S.C. 442(d)).

(b) COORDINATION WITHIN DEPARTMENT OF HOMELAND SECURITY.—The Secretary shall—

(1) ensure coordination between the Department official directly responsible for the implementation of the SAFETY Act, the Chief Procurement Officer of the Department, the Under Secretary for Science and Technology, the Under Secretary for Policy, and the Department of Homeland Security General Counsel to maximize the application and utilization of the litigation and risk management provisions of the SAFETY Act to qualified anti-terrorism technologies procured by the Department; and

(2) ensure coordination of the Department's efforts to promote awareness and utilization of the litigation and risk management provisions of the SAFETY Act in the procurement of qualified anti-terrorism technologies at the Federal, State, and local levels.

(c) ISSUANCE OF DEPARTMENTAL DIRECTIVE.—The Secretary of Homeland Security shall, in accordance with the final rule implementing the SAFETY Act, issue a Departmental management directive requiring appropriate coordination between Department procurement officials and the Department officials responsible for implementing the SAFETY Act in advance of and during the solicitation and evaluation of any Department procurement involving a qualified anti-terrorism technology.

(d) TRAINING.—As part of comprehensive procurement training authorized under section 301 of this Act, the Secretary of Homeland Security shall include SAFETY Act instruction for all acquisition employees and their representatives.

(e) REVIEW OF ANTI-TERRORISM ACQUISITIONS.—

(1) STUDY.—The Secretary of Homeland Security shall conduct a study of all Department of Homeland Security procurements, including ongoing procurements and anticipated procurements, to—

(A) identify such procurements that involve any product, equipment, service (including support and systems integration services), device, or technology (including information technology) that is being designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, deterring, or responding to acts of terrorism or limiting the harm such acts might otherwise cause; and

(B) assess whether any such product, equipment, service (including support and systems integration services), device, or technology (including information technology) is appropriate for the litigation and risk management protections of the SAFETY Act.

(2) SUMMARY AND CLASSIFICATION REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the appropriate congressional committees a report containing the findings of the study under paragraph (1). Such report shall provide for a plan for ensuring that any product, equipment, service (including support and systems integration services), device, or technology (including information technology) that is assessed as appropriate for litigation and risk management protection under the SAFETY Act shall be promptly considered for such protections.

SEC. 304. COMPTROLLER GENERAL REPORT ON DEPARTMENT OF HOMELAND SECURITY CONTRACTING.

Not later than 6 months after the date of the enactment of this Act, the Comptroller General shall submit to Congress a report on the contracting processes of the Department of Homeland Security. The report shall contain the findings of the Comptroller General with respect to any improvements in such processes that could be made through the use of new technologies.

SEC. 305. CONTRACTING REQUIREMENTS.

(a) ATTESTATION REQUIRED.—The Secretary of Homeland Security shall require any offeror for any Department of Homeland Security contract to submit as part of the offeror's bid for such a contract an attestation that affirmatively discloses any

substantial role the offeror or the offeror's company or employees may have played in creating a solicitation, request for proposal, statement of work or statement of objectives (as those terms are defined in the Federal Acquisition Regulation) for the Department of Homeland Security.

(b) ADDITIONAL REQUIREMENTS FOR CERTAIN OFFERORS.—If an offeror submits an attestation under subparagraph (a) that discloses that the offeror played a substantial role in creating a solicitation, request for proposal, statement of work or statement of objectives, for the Department of Homeland Security, the Secretary of Homeland Security shall require the offeror to submit to the Secretary a description of the safeguards used to ensure that precautions were in place to prevent the offeror from receiving information through such role that could be used to provide the offeror an undue advantage in submitting an offer for a contract.

SEC. 306. CERTIFICATION REQUIREMENTS FOR OFFERORS FOR DEPARTMENT OF HOMELAND SECURITY CONTRACTS.

(a) CERTIFICATION IN WRITING.—The Secretary of Homeland Security shall require an offeror for any contract of the Department of Homeland Security to submit as part of the offeror's bid for such a contract a certification in writing that, as of the date on which the certification is submitted, the offeror—

(1) is not in default on any payment of any tax to the Federal Government; and

(2) does not owe the Federal Government for any payment of any delinquent tax.

(b) ATTESTATION.—Nothing in this section shall prevent the Department from awarding a contract to an offeror whose attestation falls under this section.

SEC. 307. CONTRACTS FOR ASSISTANCE ACTIVITIES RELATING TO ACTS OF TERRORISM, NATURAL DISASTERS, AND OTHER EMERGENCIES.

(a) IN GENERAL.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.) is amended by redesignating section 510, relating to urban and other high risk area communications capabilities, as section 511 and by adding at the end the following:

"SEC. 512. CONTRACTS FOR ASSISTANCE ACTIVITIES RELATING TO ACTS OF TERRORISM, NATURAL DISASTERS, AND OTHER EMERGENCIES.

"(a) USE OF LOCAL FIRMS.—In entering into contracts and other agreements for debris clearance, distribution of supplies, reconstruction, and other assistance activities relating to an act of terrorism, natural disaster, or other emergency, the Secretary or the head of any component of the Department shall work toward a goal of awarding not less than 20 percent of the total value of the contracts and other agreements to qualified firms located in a county, parish, or equivalent division of general local government within the affected area.

"(b) LIMITATION.—A goal established under this section shall apply only to the extent that the goal does not interfere with the ability of the Department to provide timely and effective assistance.

"(c) PREFERENCE FOR SMALL BUSINESS CONCERNS.—In entering into contracts and other agreements described in subsection (a), the Secretary or the head of any component of the Department shall give preference to small business concerns, socially and economically disadvantaged small business concerns, small business concerns owned and controlled by service-disabled veterans, and HUBZone small business concerns (as those terms are defined in the Small Business Act (15 U.S.C. 631 et seq.)).

"(d) PRENEGOTIATED CONTRACTS.—In order to increase the use of local firms in contracts and other agreements described in subsection (a), the Secretary shall encourage the components of the Department, as well as appropriate State and local government agencies, to competitively bid and negotiate contracts and prices for services, including debris clearance, distribution of supplies, reconstruction, and other assistance, in advance of an act of terrorism, natural disaster, or other emergency.".

(b) CONFORMING AMENDMENT.—The table of contents contained in section 1(b) of such Act is amended by inserting after the item relating to section 509 the following:

"Sec. 510. Procurement of security countermeasures for strategic national stockpile.
"Sec. 511. Urban and other high risk area communications capabilities.
"Sec. 512. Contracts for assistance activities relating to acts of terrorism, natural disasters, and other emergencies.".

SEC. 308. EMERGENCY CONTRACTING SUPPORT ANNEX.

(a) ESTABLISHMENT OF SUPPORT ANNEX.—The Secretary of Homeland Security shall modify the National Response Plan to establish a Support Annex on "Emergency Contracting". The Support Annex shall set forth plans and protocols for inci-

dent-related contracting to meet urgent needs efficiently and effectively, without duplication, and in a manner designed to prevent waste, fraud and abuse.

(b) REQUIREMENTS.—The Support Annex established under subsection (a) shall—

(1) provide an overview of the framework needed to ensure adequate surge capacity for procurement activities of the Federal Government during Incidents of National Significance;

(2) identify existing contracts and contract vehicles across the Federal Government that can be used to purchase goods and services required before, during, and after an Incident of National Significance;

(4) provide a process to ensure that Federal agencies, to the greatest extent possible, competitively bid and negotiate contracts for services including debris removal, supply distribution, reconstruction, and other assistance prior to an Incident of National Significance;

(5) provide a process to ensure that the preference for the use of local contractors, as set forth in the Robert T. Stafford Disaster Relief and Emergency Assistance Act, is followed to the maximum extent practicable;

(6) provide a process for ensuring oversight of emergency contracting to detect and prevent waste, fraud, and abuse; and

(7) provide a mechanism for ensuring coordination and cooperation of contracting officers from all appropriate Federal agencies.

SEC. 309. INCREASED INSPECTOR GENERAL OVERSIGHT.

Of the amount authorized under section 101 for fiscal year 2007, $108,685,000 is for the Office of Inspector General of the Department of Homeland Security for that fiscal year.

SEC. 310. PURCHASE CARDS.

The Department of Homeland Security shall, within 30 days after the date of the enactment of this Act, review and strengthen the policy and issue Department-wide guidance governing the use of purchase cards provided by the Department to its employees for use in conducting official business. That policy or guidance must be distributed to each employee who possesses or is entitled to possess a purchase card provided by the Department. Upon issuance of the policy or guidance governing the use of purchase cards, the Department shall ensure that all employees are informed of this policy or guidance and the restrictions that apply to the use of purchase cards to prevent fraud and abuse.

TITLE IV—PERSONNEL AUTHORITIES

Subtitle A—Workforce Enhancements

SEC. 401. COST-EFFECTIVE TRAINING FOR BORDER PATROL AGENTS.

(a) IN GENERAL.—The Secretary of Homeland Security shall take such steps as may be necessary to control the costs of hiring, training, and deploying new Border Patrol agents, including—

(1) permitting individuals who are in training to become Border Patrol agents to waive certain course requirements of such training if such individuals have earlier satisfied such requirements in a similar or comparable manner as determined by the Secretary; and

(2) directing the Office of Inspector General to conduct a review of the costs and feasibility of training new Border Patrol agents at Federal training centers, including the Federal Law Enforcement Training Center facility in Charleston, South Carolina, and the HAMMER facility in Hanford, Washington, and at training facilities operated by state and local law enforcement academies, nonprofit entities, and private entities, as well as the use of all of the above to conduct portions of such training.

(b) LIMITATION ON PER-AGENT COST OF TRAINING.—

(1) IN GENERAL.—Except as provided in paragraph (2), the Secretary shall take such steps as may be necessary to ensure that the fiscal year 2007 per-agent cost of hiring, training, and deploying each new Border Patrol agent does not exceed $150,000.

(2) EXCEPTION AND CERTIFICATION.—

(A) IN GENERAL.—If the Secretary determines that the per-agent cost referred to in paragraph (1) exceeds $150,000, the Secretary shall promptly submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a certification explaining why such per-agent cost exceeds such amount.

(B) TEMPORARY SUSPENSION OF TRAINING.—Until the Secretary receives from the committees specified in subparagraph (A) an approval with respect to such increased per-agent cost, the Secretary shall suspend any new hiring, training, and deploying of Border Patrol agents.

SEC. 402. CONTINUATION OF FEDERAL LAW ENFORCEMENT TRAINING CENTER AUTHORITY TO APPOINT AND MAINTAIN A CADRE OF FEDERAL ANNUITANTS TO SUPPORT TRAINING.

Section 1202(a) of the 2002 Supplemental Appropriations Act for Further Recovery From and Response To Terrorist Attacks on the United States (42 U.S.C. 3771 note) is amended in the first sentence—

(1) by striking "enactment of this Act" and inserting "enactment of the Department of Homeland Security Authorization Act for Fiscal Year 2007"; and

(2) by striking "250" and inserting "350".

SEC. 403. CANINE DETECTION TEAM COORDINATION AND CERTIFICATION.

(a) IN GENERAL.—The Homeland Security Act of 2002 is amended by adding at the end the following:

"TITLE XVIII—MISCELLANEOUS PROVISIONS

"Subtitle A—Canine Detection Teams

"SEC. 1801. COORDINATION AND ENHANCEMENT OF CANINE DETECTION TEAM TRAINING.

"The Secretary shall—

"(1) fully coordinate the canine training programs of the Department that support the Department's counter-terrorism, counter-smuggling, transportation security, and border security missions and other missions of the Department, including, with respect to the research and development of new canine training methods, the optimum number and type of training aids, and measurements for efficiency and effectiveness;

"(2) ensure that the Department is maximizing its use of existing training facilities and resources to train canines throughout the year; and

"(3) coordinate the use of detection canines trained by other Federal agencies, nonprofit organizations, universities, and private training facilities in order to increase the number of trained detection canines available to Federal, State, and local law enforcement agencies.

"SEC. 1802. CANINE PROCUREMENT.

"The Secretary shall—

"(1) make it a priority to increase the number of domestically bred canines used by the Department to assist in its counter-terrorism mission, including the protection of ports of entry and along the United States border;

"(2) increase the utilization of domestically bred canines from universities and private and nonprofit sources in the United States; and

"(3) consult with other Federal, State, and local agencies, nonprofit organizations, universities, and private entities that use detection canines, such as those participating in the Scientific Working Group of Dog and Orthogonal Detectors (popularly known as 'SWGDOG'), as well as the Office of Management and Budget, to encourage domestic breeding of canines and consolidate canine procurement, where possible, across the Federal Government to reduce the cost of purchasing canines.

"SEC. 1803. DOMESTIC CANINE BREEDING GRANT PROGRAM.

"(a) ESTABLISHMENT OF PROGRAM.—The Secretary shall establish a competitive grant program for domestic breeders of canines. The purpose of the grant program shall be to encourage the development and growth of canine breeds that are best suited for detection training purposes within the United States and to encourage the development of applied research into enhancement of working dog performance and health traits.

"(b) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $3,000,000 for each of fiscal years 2007 through 2011.

"SEC. 1804. HOMELAND SECURITY CANINE DETECTION ACCREDITATION BOARD.

"(a) ESTABLISHMENT OF ACCREDITATION BOARD.—

"(1) IN GENERAL.—Not later than 180 days after the date on which the national voluntary consensus standards referred to in subsection (b)(1) are issued, the Secretary, in consultation with the Secretary of Defense, the Secretary of State, and the Attorney General, shall establish a Homeland Security Canine

Detection Accreditation Board to develop and implement a process for certifying compliance with such standards.

"(2) MEMBERSHIP.—The membership of the Accreditation Board shall consist of experts in the fields of canine training and explosives detection from Federal and State agencies, universities, other research institutions, and the private sector, such as those represented on the Executive Board of SWGDOG.

"(b) ACCREDITATION PROCESS.—The Accreditation Board shall establish and implement a voluntary accreditation process to—

"(1) certify that persons conducting certification of canine detection teams appropriately ensure that the canine detection teams meet the national voluntary consensus standards developed by SWGDOG;

"(2) ensure that canine detection teams do not put public safety and the safety of law enforcement personnel at risk due to fraud or weaknesses in the initial or maintenance training curriculum; and

"(3) maintain and update a public list of entities accredited by the Department to certify canine detection teams.

"(c) COMPLIANCE WITH STANDARDS.—Beginning not later than the date that is 180 days after the date on which the standards referred to in subsection (b)(1) are issued, the Secretary shall require that grant funds administered by the Department may not be used to acquire a canine detection team unless—

"(1) the canine detection team is certified under the process established under subsection (b); or

"(2) the Secretary determines that the applicant has shown special circumstances that justify the acquisition of canines that are not certified under the process established under subsection (b).

"SEC. 1805. DEFINITIONS.

"In this subtitle:

"(1) CANINE DETECTION TEAM.—The term 'canine detection team' means a canine and a canine handler.

"(2) CERTIFYING ENTITY.—The term 'certifying entity' means an entity that oversees the processes and procedures used to train and test canine detection teams.

"(3) SWGDOG.—The term 'SWGDOG' means the Scientific Working Group of Dog and Orthogonal Detectors.".

(b) CLERICAL AMENDMENT.—The table of sections in section 1(b) of such Act is amended by adding at the end the following:

"TITLE XVIII—MISCELLANEOUS PROVISIONS

"Subtitle A—Canine Detection Teams

"Sec. 1801. Coordination and enhancement of canine detection team training.
"Sec. 1802. Canine procurement.
"Sec. 1803. Domestic canine breeding grant program.
"Sec. 1804. Homeland Security Canine Detection Accreditation Board.
"Sec. 1805. Definitions.".

(c) REPORT.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Homeland Security shall report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on the plan of the Secretary to coordinate and consolidate the canine training programs of the Department of Homeland Security in accordance with section 1801 of the Homeland Security Act of 2002, as added by subsection (b).

SEC. 404. AUTHORITY FOR CUSTOMS AND BORDER PROTECTION TO APPOINT AND MAINTAIN A CADRE OF FEDERAL ANNUITANTS.

(a) IN GENERAL.—Notwithstanding any other provision of law, the Commissioner of United States Customs and Border Protection (CBP) may, for a period ending not later than five years after the date of the enactment of this Act, appoint and employ up to 500 Federal annuitants to any position in CBP that supports the acceleration of the ability of CBP to secure the international land and maritime borders of the United States—

(1) without regard to any provision of title 5, United States Code, which might otherwise require the application of competitive hiring procedures; and

(2) who shall not be subject to any reduction in pay (for annuity allocable to the period of actual employment) under the provisions of section 8344 or 8468 of such title or similar provision of any other retirement system for employees.

(b) UTILIZATION.—The authority granted to the Commissioner of United States Customs and Border Protection under subsection (a) shall cease 5 years after the date of enactment of this Act, at which point, the employment of annuitants under this authority shall cease.

(c) RULE OF CONSTRUCTION.—A reemployed Federal annuitant as to whom a waiver of reduction under subsection (a)(2) applies shall not, for any period during which such waiver is in effect, be considered an employee for purposes of subchapter III of chapter 83 or chapter 84 of title 5, United States Code, or such other retirement system (referred to in such subsection) as may apply.

(d) NO DISPLACEMENT.—No appointment under this section may be made if such appointment would result in the displacement of any employee.

(e) COUNTING.—The counting of Federal annuitants shall be done on a full-time equivalent basis.

(f) DEFINITIONS.—For purposes of this section:

(1) FEDERAL ANNUITANT.—The term "Federal annuitant" means an employee who has retired under the Civil Service Retirement System, the Federal Employees' Retirement System, or any other retirement system for Federal employees.

(2) EMPLOYEE.—The term "employee" has the meaning given such term in section 2105 of title 5, United States Code.

SEC. 405. STRENGTHENING BORDER PATROL RECRUITMENT AND RETENTION.

In order to address the recruitment and retention challenges faced by United States Customs and Border Protection, the Secretary of Homeland Security shall establish a plan, consistent with existing Federal statutes applicable to pay, recruitment, relocation, and retention of Federal law enforcement officers. Such plan shall include the following components:

(1) The establishment of a recruitment incentive for Border patrol agents, including the establishment of a foreign language incentive award.

(2) The establishment of a retention plan, including the payment of bonuses to Border Patrol agents for every year of service after the first two years of service.

(3) An increase in the pay percentage differentials to Border Patrol agents in certain high-cost areas, as determined by the Secretary, consistent with entry-level pay to other Federal, State, and local law enforcement agencies.

(4) The establishment of a mechanism whereby Border Patrol agents can transfer from one location to another after the first two years of service in their initial duty location.

SEC. 406. CUSTOMS AND BORDER PROTECTION OFFICER PAY EQUITY.

(a) DEFINITIONS.—For purposes of this section:

(1) The term "Government retirement system" means a retirement system established by law for employees of the Government of the United States.

(2) The term "Customs and Border Protection Officer position" refers to any Customs and Border Protection Officer position—

(A) which is within the Department of Homeland Security, and

(B) the primary duties of which consist of enforcing the immigration, customs, or agriculture laws of the United States;

such term includes a supervisory or administrative position within the Department of Homeland Security to which an individual transfers directly from a position described in the preceding provisions of this paragraph in which such individual served for at least 3 years.

(3) The term "law enforcement officer" has the meaning given such term under the Government retirement system involved.

(4) The term "Executive agency" or "agency" has the meaning given under section 105 of title 5, United States Code.

(5) The term "prior qualified service" means service as a Customs and Border Protection Officer within the Department of Homeland Security, since its creation in March 2003.

(b) TREATMENT AS A LAW ENFORCEMENT OFFICER.—In the administration of any Government retirement system, service in a Customs and Border Protection Officer position shall be treated in the same way as service performed in a law enforcement officer positions, subject to succeeding provisions of this section.

(c) APPLICABILITY.—Subsection (b) shall apply in the case of—

(1) any individual first appointed to a Customs and Border Protection Officer position on or after the date of enactment of this Act; and

(2) any individual who—

(A) holds a Customs and Border Protection Officer position on the date of the enactment of this Act pursuant to an appointment made before such date; and

(B) who submits an appropriate election under this subparagraph, to the agency administering the retirement system involved, within 5 years after the date of the enactment of this Act or before separation from Government service, whichever is earlier.

(d) INDIVIDUAL CONTRIBUTIONS FOR PRIOR QUALIFIED SERVICE.—

(1) IN GENERAL.—An individual described in subsection (c)(2)(B) may, with respect to prior qualified service performed by such individual, contribute to the retirement system administered by the Department of Homeland Security (for deposit in the appropriate fund within the Treasury) the difference between the individual contributions that were actually made for such service and the individual contributions that should have been made for such service if subsection (b) had then been in effect (with interest).

(2) EFFECT OF NOT CONTRIBUTING.—If less than the full contribution under paragraph (1) is made, all prior qualified service of the individual shall remain fully creditable as law enforcement officer service, but the resulting annuity (before cost-of-living adjustments) shall be reduced in a manner such that, when combined with the unpaid amount, would result in the present value of the total being actuarially equivalent to the present value of the annuity that would otherwise have been payable if the full contribution had been made.

(e) GOVERNMENT CONTRIBUTIONS FOR PRIOR QUALIFIED SERVICE.—

(1) IN GENERAL.—If an individual makes an election under subsection (c)(2)(B), the Department of Homeland Security shall remit, with respect to any prior qualified service, the total amount of additional Government contributions that would have been required for such service under the retirement system involved if subsection (b) had then been in effect (with interest).

(2) CONTRIBUTIONS TO BE MADE RATABLY.—Government contributions under this subsection on behalf of an individual shall be made ratably (on at least an annual basis) over the 10-year period beginning on the date an individual's retirement deductions begin to be made.

(f) EXEMPTION FROM MANDATORY SEPARATION.—Effective during the 3-year period beginning on the date of enactment of this Act, nothing in this section shall result in any individual being involuntarily separated on account of the provisions of any retirement system relating to the mandatory separation of a law enforcement officer on account of age or age and service combined.

(g) RULE OF CONSTRUCTION.—Nothing in this section shall be considered to apply in the case of a reemployed annuitant.

(h) REGULATIONS.—The Secretary of Homeland Security shall issue any regulations necessary to carry out this section.

Subtitle B—Improving Security Clearance Process

SEC. 411. INCREASED SECURITY SCREENING OF HOMELAND SECURITY OFFICIALS.

(a) REVIEW REQUIRED.— Not later than 90 days after the date of enactment of this Act, the Secretary of Homeland Security shall conduct a Department-wide review of Department of Homeland Security security clearance and suitability review procedures for Department employees and contractors, as well as individuals in state and local government agencies and private sector entities with a need to receive classified information.

(b) STRENGTHENING OF SECURITY SCREENING POLICIES.—

(1) IN GENERAL.—Based on the findings of the review conducted under subsection (a), the Secretary shall, as appropriate, take all necessary steps to strengthen the Department's security screening policies, including consolidating the security clearance investigative authority at the Departmental Headquarters.

(2) ELEMENTS.—In strengthening security screening policies under paragraph (1), the Secretary shall consider whether and where appropriate ensure that—

(A) all components of the Department of Homeland Security meet or exceed Federal and Departmental standards for security clearance investigations, adjudications, and suitability reviews;

(B) the Department has a cadre of well-trained adjudicators; and that the Department has in place a program to train and oversee adjudicators; and

(C) suitability reviews are conducted for all Department of Homeland Security employees who transfer from a component of the Department to Departmental Headquarters.

SEC. 412. AUTHORITIES OF CHIEF SECURITY OFFICER.

(a) ESTABLISHMENT.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.) is amended by adding at the end the following:

"SEC. 707. CHIEF SECURITY OFFICER.

"(a) ESTABLISHMENT.—There is in the Department a Chief Security Officer.

"(b) RESPONSIBILITIES.—The Chief Security Officer shall—

"(1) have responsibility for personnel security, facility access, security awareness, and related training;

"(2) ensure that each component of the Department complies with Federal standards for security clearances and background investigations;

"(3) ensure, to the greatest extent practicable, that individuals in state and local government agencies and private sector entities with a need to receive classified information, receive the appropriate clearances in a timely fashion; and

"(4) perform all other functions as determined by the Secretary.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the item relating to section 706 the following new item:

"Sec. 707. Chief Security Officer.".

TITLE V—INTELLIGENCE AND INFORMATION SHARING

SEC. 501. DEPARTMENTAL REORGANIZATION.

(a) REDESIGNATION OF DIRECTORATE FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION AS OFFICE OF INTELLIGENCE AND ANALYSIS.—Section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121) is amended—

(1) in subsection (a)(1)—

(A) by striking "a Directorate for Information Analysis and Infrastructure Protection" and inserting "an Office of Intelligence and Analysis"; and

(B) by striking "an Under Secretary for Information Analysis and Infrastructure Protection" and inserting "an Under Secretary for Intelligence and Analysis";

(2) by striking subsection (b) and redesignating subsections (c) through (g) as subsections (b) through (f), respectively;

(3) in subsection (b), as so redesignated—

(A) by striking "and infrastructure protection" and inserting "and intelligence"; and

(B) by striking "the Under Secretary for Information Analysis and Infrastructure Protection" and inserting "the Under Secretary for Intelligence and Analysis";

(4) in subsection (c), as so redesignated—

(A) by striking "the Under Secretary for Information Analysis and Infrastructure Protection" and inserting "the Under Secretary for Intelligence and Analysis";

(B) by striking paragraphs (2), (5), and (6), and redesignating paragraphs (3), (4), (7), (8), (9), (10), (11), (12), (13), (14), (15), (16), and (17) as paragraphs (2) through (14), respectively;

(C) by redesignating paragraphs (18) and (19) as paragraphs (20) and (21), respectively;

(D) in paragraph (2), as so redesignated, by striking "To integrate" and inserting "To participate in the integration of";

(E) in paragraph (14), as so redesignated, by inserting "the Assistant Secretary for Infrastructure Protection and" after "coordinate with"; and

(F) by inserting after paragraph (14), as redesignated by subparagraph (B), the following new paragraphs:

"(15) To coordinate and enhance integration among intelligence components of the Department.

"(16) To establish intelligence priorities, policies, processes, standards, guidelines, and procedures for the Department.

"(17) To establish a structure and process to support the missions and goals of the intelligence components of the Department.

"(18) To ensure that, whenever possible—

"(A) the Under Secretary for Intelligence and Analysis produces and disseminates reports and analytic products based on open-source information that do not require a national security classification under applicable law; and

"(B) such unclassified open-source reports are produced and disseminated contemporaneously with reports or analytic products concerning the same or similar information that the Under Secretary for Intelligence and Analysis produces and disseminates in a classified format.

"(19) To establish within the Office of Intelligence and Analysis an Internal Continuity of Operations (COOP) Plan that—

"(A) assures that the capability exists to continue uninterrupted operations during a wide range of potential emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies, that is maintained at a high level of readiness and is capable of implementation with and without warning; and

"(B) includes plans and procedures governing succession to office within the Office of Intelligence and Analysis, including—

"(i) emergency delegations of authority (where permissible, and in accordance with applicable law);

"(ii) the safekeeping of vital resources, facilities, and records;

"(iii) the improvisation or emergency acquisition of vital resources necessary for the performance of operations of the Office; and

"(iv) the capability to relocate essential personnel and functions to and to sustain the performance of the operations of the Office at an alternate work site until normal operations can be resumed.";

(5) in subsections (d) and (e), as redesignated by subsection (a)(2), by striking "Directorate" each place it appears and inserting "Office"; and

(6) in subsection (f), as redesignated by subsection (a)(2)—

(A) by striking "the Under Secretary for Information Analysis and Infrastructure Protection" and inserting "the Under Secretary for Intelligence and Analysis and the Assistant Secretary for Infrastructure Protection"; and

(B) by inserting "and section 203" after "under this section".

(b) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) HOMELAND SECURITY ACT.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(A) in section 103(a)(2), by striking "Information Analysis and Infrastructure Protection" and inserting "Intelligence and Analysis";

(B) in section 223, by striking "Under Secretary for Information Analysis and Infrastructure Protection" and inserting "Under Secretary for Intelligence and Analysis, in cooperation with the Assistant Secretary for Infrastructure Protection";

(C) in section 224, by striking "Under Secretary for Information Analysis and Infrastructure Protection" and inserting "Assistant Secretary for Infrastructure Protection";

(D) in section 302(3), by striking "Under Secretary for Information Analysis and Infrastructure Protection" and inserting "Under Secretary for Intelligence and Analysis and the Assistant Secretary for Infrastructure Protection"; and

(E) in subsection (d) of section 510—

(i) in paragraph (1), by striking "Directorate for Information Analysis and Infrastructure Protection" and inserting "Office of Intelligence and Analysis"; and

(ii) in paragraph (2), by striking "Under Secretary for Information Analysis and Infrastructure Protection" and inserting "Under Secretary for Intelligence and Analysis".

(2) HEADINGS.—

(A) SECTION 201.—The heading for section 201 of such Act is amended to read as follows:

"SEC. 201. OFFICE OF INTELLIGENCE AND ANALYSIS.".

(B) SECTION 201(a).—The heading for subsection (a) of section 201 of such Act is amended to read as follows:

"(a) UNDER SECRETARY OF HOMELAND SECURITY FOR INTELLIGENCE AND ANALYSIS.—".

(C) SECTION 201(b).—The heading for subsection (b) of section 201 of such Act, as redesignated by subsection (a)(2), is amended to read as follows:

"(b) DISCHARGE OF INTELLIGENCE AND ANALYSIS.—".

(3) NATIONAL SECURITY ACT OF 1947.—Section 106(b)(2)(I) of the National Security Act of 1947 (50 U.S.C. 403–6) is amended to read as follows:

"(I) The Under Secretary of Homeland Security for Intelligence and Analysis.".

(4) INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004.—Section 7306(a)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458; 118 Stat. 3848) is amended by striking "Under Secretary for Information Analysis and Infrastructure Protection" and inserting "Under Secretary for Intelligence and Analysis".

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the item relating to section 201 and inserting the following:

"Sec. 201. Office of Intelligence and Analysis.".

SEC. 502. INTELLIGENCE COMPONENTS OF DEPARTMENT OF HOMELAND SECURITY.

(a) RESPONSIBILITIES.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 201 et seq.) is amended by adding at the end the following new section:

"SEC. 203. INTELLIGENCE COMPONENTS.

"(a) RESPONSIBILITIES.—Subject to the direction and control of the Secretary, the responsibilities of the head of each intelligence component of the Department are as follows:

"(1) To ensure that duties related to the acquisition, analysis, and dissemination of homeland security information are carried out effectively and efficiently in support of the Under Secretary for Intelligence and Analysis.

"(2) To support and implement the goals established in cooperation with the Under Secretary for Intelligence and Analysis.

"(3) To incorporate the input of the Under Secretary for Intelligence and Analysis with respect to performance appraisals, bonus or award recommendations, pay adjustments, and other forms of commendation.

"(4) To coordinate with the Under Secretary for Intelligence and Analysis in the recruitment, establishment of core competency standards, and selection of intelligence officials of the intelligence component.

"(5) To advise and coordinate with the Under Secretary for Intelligence and Analysis on any plan to reorganize or restructure the intelligence component that would, if implemented, result in realignments of intelligence functions.

"(6) To ensure that employees of the intelligence component have knowledge of and comply with the programs and policies established by the Under Secretary for Intelligence and Analysis and other appropriate officials of the Department and that such employees comply with all applicable laws and regulations.

"(7) To perform such other duties relating to such responsibilities as the Secretary may provide.

"(b) TRAINING OF EMPLOYEES.—The Secretary shall provide training and guidance for employees, officials, and senior executives of the intelligence components of the Department to develop knowledge of laws, regulations, operations, policies, procedures, and programs that are related to the functions of the Department relating to the handling, analysis, dissemination, and collection of homeland security information.".

(b) INTELLIGENCE COMPONENT DEFINED.—Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) is amended by adding at the end the following new paragraph:

"(17) The term 'intelligence component of the Department' means any directorate, agency, or element of the Department that gathers, receives, analyzes, produces, or disseminates homeland security information except—

"(A) a directorate, agency, or element of the Department that is required to be maintained as a distinct entity under this Act; or

"(B) any personnel security, physical security, document security, or communications security program within any directorate, agency, or element of the Department.".

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 202 the following:

"Sec. 203. Intelligence components.".

SEC. 503. HOMELAND SECURITY ADVISORY SYSTEM.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 is further amended—

(1) in section 201(c)(4), as redesignated by section 501, by inserting "under section 204" after "Homeland Security Advisory System"; and

(2) by adding at the end the following:

"SEC. 204. HOMELAND SECURITY ADVISORY SYSTEM.

"(a) REQUIREMENT.—The Under Secretary for Intelligence and Analysis shall implement a Homeland Security Advisory System in accordance with this section to provide public advisories and alerts regarding threats to homeland security, including national, regional, local, and economic sector advisories and alerts, as appropriate.

"(b) REQUIRED ELEMENTS.—The Under Secretary, in each advisory or alert issued under the System, shall—

"(1) include information on appropriate protective measures and countermeasures that may be taken in response to the threat;

"(2) whenever possible, limit the scope of the advisory or alert to a specific region, locality, or economic sector believed to be at risk; and

"(3) not use color designations as the exclusive means of specifying the homeland security threat conditions that are the subject of the advisory or alert.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 203 (as added by section 502(c)) the following:

"Sec. 204. Homeland Security Advisory System.".

SEC. 504. HOMELAND SECURITY INFORMATION SHARING.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is further amended by adding at the end the following:

"SEC. 205. HOMELAND SECURITY INFORMATION SHARING.

"(a) INFORMATION SHARING ENVIRONMENT.—Consistent with section 1016 of the National Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), the Secretary shall integrate and standardize the information of the intelligence components of the Department into a Department information sharing environment, to be administered by the Under Secretary for Intelligence and Analysis.

"(b) INFORMATION SHARING AND KNOWLEDGE MANAGEMENT OFFICERS.—For each intelligence component of the Department, the Secretary shall designate an information sharing and knowledge management officer who shall report to the Under Secretary for Intelligence and Analysis with respect to coordinating the different systems used in the Department to gather and disseminate homeland security information.

"(c) STATE, LOCAL, TRIBAL, AND PRIVATE-SECTOR SOURCES OF INFORMATION.—

"(1) ESTABLISHMENT OF BUSINESS PROCESSES.—The Under Secretary for Intelligence and Analysis shall establish Department-wide procedures for the review and analysis of information gathered from State, local, tribal, and private-sector sources and, as appropriate, integrate such information into the information gathered by the Department and other departments and agencies of the Federal Government.

"(2) FEEDBACK.—The Secretary shall develop mechanisms to provide analytical and operational feedback to any State, local, tribal and private-sector entities that gather information and provide such information to the Secretary.

"(d) TRAINING AND EVALUATION OF EMPLOYEES.—

"(1) TRAINING.—The Under Secretary shall provide to employees of the Department opportunities for training and education to develop an understanding of the definition of homeland security information, how information available to them as part of their duties might qualify as homeland security information, and how information available to them is relevant to the Office of Intelligence and Analysis.

"(2) EVALUATIONS.—The Under Secretary shall, on an ongoing basis, evaluate how employees of the Office of Intelligence and Analysis and the intelligence components of the Department are utilizing homeland security information and participating in the Department information sharing environment.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by adding after the item relating to section 204 (as added by section 503(b)) the following:

"Sec. 205. Homeland security information sharing.".

(c) ESTABLISHMENT OF COMPREHENSIVE INFORMATION TECHNOLOGY NETWORK ARCHITECTURE.—

(1) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following new section:

"SEC. 206. COMPREHENSIVE INFORMATION TECHNOLOGY NETWORK ARCHITECTURE.

"(a) ESTABLISHMENT.—The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall establish a comprehensive information technology network architecture for the Office of Intelligence and Analysis.

"(b) NETWORK MODEL.—The comprehensive information technology network architecture established under subsection (a) shall, to the extent possible, incorporate the approaches, features, and functions of on the network proposed by the Markle Foundation in reports issued in October 2002 and December 2003, known as the System-wide Homeland Security Analysis and Resource Exchange (SHARE) Network.

"(c) COMPREHENSIVE INFORMATION TECHNOLOGY NETWORK ARCHITECTURE DEFINED.—the term 'comprehensive information technology network architecture'

means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the strategic goals and information resources management goals of the Office of Intelligence and Analysis.".

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 205 (as added by section 504(b)) the following:

"Sec. 206. Comprehensive information technology network architecture.".

(3) REPORTS.—

(A) REPORT ON IMPLEMENTATION OF PLAN.—Not later than 360 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report containing a plan to implement the comprehensive information technology network architecture for the Office of Intelligence and Analysis of the Department of Homeland Security required under section 206 of the Homeland Security Act of 2002, as added by paragraph (1). Such report shall include the following:

(i) Priorities for the development of the comprehensive information technology network architecture and a rationale for such priorities.

(ii) An explanation of how the various components of the comprehensive information technology network architecture will work together and interconnect.

(iii) A description of the technology challenges that the Office of Intelligence and Analysis will face in implementing the comprehensive information technology network architecture.

(iv) A description of technology options that are available or are in development that may be incorporated into the comprehensive technology network architecture, the feasibility of incorporating such options, and the advantages and disadvantages of doing so.

(v) An explanation of any security protections to be developed as part of the comprehensive information technology network architecture.

(vi) A description of any safeguards for civil liberties and privacy to be built into the comprehensive information technology network architecture.

(vii) An operational best practices plan.

(B) PROGRESS REPORT.—Not later than 180 days after the date on which the report is submitted under subparagraph (A), the Secretary of Homeland Security shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the progress of the Secretary in developing the comprehensive information technology network architecture required under section 206 of the Homeland Security Act of 2002, as added by paragraph (1).

SEC. 505. STATE, LOCAL, TRIBAL, AND REGIONAL INFORMATION FUSION CENTER INITIATIVE.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is further amended by adding at the end the following:

"SEC. 207. STATE, LOCAL, TRIBAL, AND REGIONAL INFORMATION FUSION CENTER INITIATIVE.

"(a) ESTABLISHMENT.—The Secretary shall establish a State, Local, and Tribal Information Fusion Center Initiative to establish partnerships with State, local, tribal, and regional information fusion centers.

"(b) DUTIES.—Through the State, Local, Tribal, and Regional Information Fusion Center Initiative, the Secretary shall—

"(1) coordinate with the principal official of each State, local, tribal, or regional information fusion center and the official designated as the Homeland Security Advisor of the State;

"(2) provide Department operational and intelligence advice and assistance to State, local, tribal, and regional information fusion centers;

"(3) support efforts to include State, local, tribal, and regional information fusion centers into efforts to establish an information sharing environment (as defined under section 1016(2) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458; 118 Stat. 3665));

"(4) conduct table-top and live training exercises to regularly assess the capability of individual and regional networks of State, local, tribal, and regional information fusion centers to integrate the efforts of such networks with the efforts of the Department;

"(5) coordinate with other relevant Federal entities engaged in homeland security-related activities;

"(6) provide analytic and reporting advice and assistance to State, local, tribal, and regional information fusion centers;

"(7) review homeland security information gathered by State, local, tribal, and regional information fusion centers and incorporate relevant information with homeland security information of the Department;

"(8) Provide management assistance to State, local, tribal, and regional information fusion centers;

"(9) Serve as a point of contact to ensure the dissemination of relevant homeland security information.

"(10) facilitate close communication and coordination between State, local, tribal, and regional information fusion centers and the Department;

"(11) provide State, local, tribal, and regional information fusion centers with expertise on Department resources and operations;

"(12) provide training to State, local, tribal, and regional information fusion centers and encourage such information fusion centers to participate in terrorist threat-related exercises conducted by the Department; and

"(13) carry out such other duties as the Secretary determines are appropriate.

"(c) DEFINITION OF STATE, LOCAL, TRIBAL, OR REGIONAL INFORMATION FUSION CENTER.—For purposes of this section, the term 'State, local, tribal, or regional information fusion center' means a local or regional center comprised of State, local, or tribal governmental entities that—

"(1) serves as a data analysis and dissemination center for potentially relevant homeland security information;

"(2) is managed by a state, local, or tribal government entity; or

"(3) is designated as a State, local, tribal, or regional information fusion center by the Secretary.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by adding after the item relating to section 206 (as added by section 504(c)(2)) the following:

"Sec. 207. State, Local, Tribal, and Regional Information Fusion Center Initiative.".

(c) REPORTS.—

(1) CONCEPT OF OPERATIONS.—Not later than 90 days after the date of the enactment of this Act and before the State, Local, Tribal, and Regional Information Fusion Center Initiative under section 207 of the Homeland Security Act of 2002, as added by subsection (a), has been implemented, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that contains a concept of operations for the Initiative, which shall include a privacy and civil liberties impact assessment.

(2) PRIVACY AND CIVIL LIBERTIES.—

(A) REVIEW OF CONCEPT OF OPERATIONS.—Not later than 180 days after the date on which the report under paragraph (1) is submitted, the Privacy Officer of the Department of Homeland Security and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security shall review the privacy and civil liberties implications of the Initiative and the concept of operations and report any concerns to the Secretary of Homeland Security and the Under Secretary of Homeland Security for Intelligence and Analysis.

(B) REVIEW OF PRIVACY IMPACT.—Under the authority of section 222(5) of the Homeland Security Act of 2002 (6 U.S.C. 142(5)), not later than one year after the date on which the State, Local, Tribal, and Regional Information Fusion Center Initiative is implemented, the Privacy Officer of the Department of Homeland Security, in consultation with the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security, shall submit to Congress, the Secretary of Homeland Security, and the Under Secretary of Homeland Security for Intelligence and Analysis a report on the privacy and civil liberties impact of the Initiative.

SEC. 506. HOMELAND SECURITY INFORMATION SHARING FELLOWS PROGRAM.

(a) ESTABLISHMENT OF PROGRAM.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is further amended by adding at the end the following:

"SEC. 208. HOMELAND SECURITY INFORMATION SHARING FELLOWS PROGRAM.

"(a) ESTABLISHMENT.—

"(1) IN GENERAL.—The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall establish a fellowship program in accordance with this section for the purpose of—

"(A) detailing State, local, and tribal analysts and law enforcement officials and officers to the Department to participate in the work of the Office of Intelligence and Analysis in order to become familiar with—

"(i) the mission and capabilities of the Office of Intelligence and Analysis; and

"(ii) the role, programs, products, and personnel of the Office of Intelligence and Analysis; and

"(B) promoting information sharing between the Department and State, local, and tribal analysts and law enforcement agencies by stationing analysts and law enforcement officers alongside Department intelligence analysts in order to—

"(i) serve as a point of contact in the Department to assist in the representation of State, local, and tribal homeland security information needs;

"(ii) identify homeland security information of interest to State, local, and tribal analysts and law enforcement officers; and

"(iii) assist Department analysts in preparing and disseminating terrorism-related products that are tailored to State, local, and tribal analysts and law enforcement agencies and designed to help thwart terrorist attacks.

"(2) PROGRAM NAME.—The program under this section shall be known as the 'Homeland Security Information Sharing Fellows Program'.

"(b) ELIGIBILITY.—

"(1) IN GENERAL.—In order to be eligible for selection as an Information Sharing Fellow under the program, an individual must—

"(A) have homeland security-related responsibilities or law enforcement-related responsibilities;

"(B) be eligible for an appropriate national security clearance;

"(C) possess a valid need for access to classified information, as determined by the Under Secretary for Intelligence and Analysis; and

"(D) be an employee of an eligible entity.

"(2) ELIGIBLE ENTITIES.—For purposes of this subsection, the term 'eligible entity' means—

"(A) a State, local, tribal, or regional fusion center;

"(B) a State or local law enforcement or other government entity that serves a major metropolitan area, as determined by the Secretary;

"(C) a State or local law enforcement or other government entity that serves a suburban or rural area, as determined by the Secretary;

"(D) a State or local law enforcement or other government entity with port responsibilities, as determined by the Secretary;

"(E) a State or local law enforcement or other government entity with border responsibilities, as determined by the Secretary;

"(F) a State or local law enforcement or other government entity with agricultural responsibilities, as determined by the Secretary;

"(G) a tribal law enforcement or other authority; or

"(H) such other entity as the Secretary determines is appropriate.

"(c) OPTIONAL PARTICIPATION.—No State, local, or tribal law enforcement or other government entity shall be required to participate in the Homeland Security Information Sharing Fellows Program.

"(d) PROCEDURES FOR NOMINATION AND SELECTION.—

"(1) IN GENERAL.—The Under Secretary shall establish procedures to provide for the nomination and selection of individuals to participate in the Homeland Security Information Sharing Fellows Program.

"(2) LIMITATIONS.—The Under Secretary shall—

"(A) select analysts and law enforcement officers representing a broad cross-section of State, local, and tribal agencies;

"(B) ensure that the number of Information Sharing Fellows selected does not impede the activities of the Office of Intelligence and Analysis; and

"(C) take reasonable steps to promote racial, ethnic, and gender diversity in the Information Sharing Fellows Program.

"(e) LENGTH OF SERVICE.—Information Sharing Fellows shall serve for a reasonable period of time, as determined by the Under Secretary. Such period of time shall be sufficient to advance the information-sharing goals of the Under Secretary and encourage participation by as many qualified nominees as possible.

"(f) CONDITION.—As a condition of selecting an individual as an Information Sharing Fellow under the program, the Under Secretary shall require that the individ-

ual's employer agree to continue to pay the individual's salary and benefits during the period for which the individual is detailed.

"(g) STIPEND.—During the period for which an individual is detailed under the program, the Under Secretary shall, subject to the availability of appropriations provide to the individual a stipend to cover the individual's reasonable living expenses for that period.

"(h) SECURITY CLEARANCES.—If an individual selected for a fellowship under the Information Sharing Fellows Program does not possess the appropriate security clearance, the Under Secretary shall ensure that security clearance processing is expedited for such individual and shall ensure that each such Information Sharing Fellow has obtained the appropriate security clearance prior to participation in the Program.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by adding after the item relating to section 207 (as added by section 505(b)) the following:

"Sec. 208. Homeland Security Information Sharing Fellows Program.".

(c) REPORTS.—

(1) CONCEPT OF OPERATIONS.—Not later than 90 days after the date of the enactment of this Act and before the Homeland Security Information Sharing Fellows Program under section 208 of the Homeland Security Act of 2002, as added by subsection (a), has been implemented, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that contains a concept of operations for the Program, which shall include a privacy and civil liberties impact assessment.

(2) PRIVACY AND CIVIL LIBERTIES.—

(A) REVIEW OF CONCEPT OF OPERATIONS.—Not later than 180 days after the date on which the report under paragraph (1) is submitted, the Privacy Officer of the Department of Homeland Security and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security shall review the privacy and civil liberties implications of the Program and the concept of operations and report any concerns to the Secretary of Homeland Security and the Under Secretary of Homeland Security for Intelligence and Analysis. The Secretary may not implement the Program until the Privacy Officer and the Officer for Civil Rights and Civil Liberties have certified that any privacy or civil liberties concerns have been addressed.

(B) REVIEW OF PRIVACY IMPACT.—Under the authority of section 222(5) of the Homeland Security Act of 2002 (6 U.S.C. 142(5)), not later than one year after the date on which the Homeland Security Information Sharing Fellows Program is implemented, the Privacy Officer of the Department of Homeland Security, in consultation with the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security, shall submit to Congress, the Secretary of Homeland Security, and the Under Secretary of Homeland Security for Intelligence and Analysis a report on the privacy and civil liberties impact of the Program.

SEC. 507. FULL AND EFFICIENT USE OF OPEN-SOURCE INTELLIGENCE.

(a) REQUIREMENT.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is further amended by adding at the end the following:

"SEC. 209. FULL AND EFFICIENT USE OF OPEN-SOURCE INTELLIGENCE.

"(a) USE BY UNDER SECRETARY.—The Secretary shall ensure that, in meeting the analytic responsibilities under section 201(d) and in formulating requirements for additional information, the Under Secretary for Intelligence and Analysis makes full and efficient use of open-source information by acquiring, gathering, processing, and analyzing open-source information to produce open-source intelligence products.

"(b) ANALYSIS PERFORMANCE.—The Secretary shall ensure that the Department makes full and efficient use of open-source information to analyze United States critical infrastructure nodes from the perspective of terrorists using publicly available information. The Secretary shall share the results of the analysis with appropriate Federal, State, local, tribal, and private-sector officials.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 208 (as added by section 506(b)) the following:

"Sec. 209. Full and efficient use of open-source intelligence.".

SEC. 508. STRENGTHENING THE CAPABILITIES OF THE HUMAN SMUGGLING AND TRAFFICKING CENTER.

(a) IN GENERAL.—The Secretary, acting through the Assistant Secretary of Homeland Security for United States Immigration and Customs Enforcement, shall provide to the Human Smuggling and Trafficking Center (in this section referred to as the "Center") the administrative support and funding required for its maintenance, including funding for personnel, leasing of office space, supplies, equipment, technology, training, and travel expenses necessary for the Center to carry out its mission.

(b) STAFFING OF THE CENTER.—

(1) IN GENERAL.—Funding provided under subsection (a) shall be used for the hiring of for not fewer than 30 full-time equivalent staff for the Center, to include the following:

(A) One Director.

(B) One Deputy Director for Smuggling.

(C) One Deputy Director for Trafficking.

(D) One Deputy Director for Terrorist Travel.

(E) Not fewer than 15 intelligence analysts or Special Agents, to include the following:

(i) Not fewer than ten such analysts or Agents shall be intelligence analysts or law enforcement agents who shall be detailed from entities within the Department of Homeland Security with human smuggling and trafficking related responsibilities, as determined by the Secretary.

(ii) Not fewer than one full time professional staff detailee from each of the United States Coast Guard, United States Immigration and Customs Enforcement, United States Customs and Border Protection, Transportation Security Administration, and the Office of Intelligence and Analysis.

(2) REQUIREMENTS.—Intelligence analysts or Special Agents detailed to the Center under paragraph (1)(E) shall have at least three years experience related to human smuggling or human trafficking.

(3) DURATION OF ASSIGNMENT.—An intelligence analyst or Special Agent detailed to the Center under paragraph (1)(E) shall be detailed for a period of not less than two years.

(c) FUNDING REIMBURSEMENT.—In operating the Center, the Secretary of Homeland Security shall act in accordance with all applicable requirements of the Economy Act (31 U.S.C. 1535), and shall seek reimbursement from the Attorney General and the Secretary of State, in such amount or proportion as is appropriate, for costs associated with the participation of the Department of Justice and the Department of State in the operation of the Center.

(d) DEVELOPMENT OF PLAN.—The Secretary of Homeland Security shall develop a plan for the Center that—

(1) defines the roles and responsibilities of each Department participating in the Center;

(2) describes how the Department of Homeland Security shall utilize its resources to ensure that the Center uses intelligence to focus and drive its efforts;

(3) describes the mechanism for the sharing of information from United States Immigration and Customs Enforcement and United States Customs and Border Protection field offices to the Center;

(4) describes the mechanism for the sharing of homeland security information from the Center to the Office of Intelligence and Analysis, including how such sharing shall be consistent with section 1016(b) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458);

(5) establishes reciprocal security clearance status to other participating agencies in the Center in order to ensure full access to necessary databases;

(6) establishes or consolidates networked systems for the Center; and

(7) ensures that the assignment of personnel to the Center from agencies of the Department of Homeland Security is incorporated into the civil service career path of such personnel.

(e) MEMORANDUM OF UNDERSTANDING.—The Secretary of Homeland Security shall execute with the Attorney General a Memorandum of Understanding in order to clarify cooperation and coordination between United States Immigration and Customs Enforcement and the Federal Bureau of Investigation regarding issues related to human smuggling, human trafficking, and terrorist travel.

(f) COORDINATION WITH THE OFFICE OF INTELLIGENCE AND ANALYSIS.—The Office of Intelligence and Analysis, in coordination with the Center, shall submit to Federal, State, local, and tribal law enforcement and other relevant agencies periodic reports regarding terrorist threats related to human smuggling, human trafficking, and terrorist travel.

(g) AUTHORIZATION OF APPROPRIATIONS.—Of the amount authorized to be appropriated under section 101 for fiscal year 2007, $10,000,000 is to carry out this section for that fiscal year.

TITLE VI—PREVENTION OF NUCLEAR AND BIOLOGICAL TERRORISM

SEC. 601. ESTABLISHMENT OF OFFICE OF DOMESTIC NUCLEAR DETECTION.

(a) ESTABLISHMENT.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended by adding at the end the following new title:

"TITLE XIX—DOMESTIC NUCLEAR DETECTION

"SEC. 1901. OFFICE OF DOMESTIC NUCLEAR DETECTION.

"(a) IN GENERAL.—There shall be in the Department of Homeland Security an Office of Domestic Nuclear Detection.

"(b) PURPOSE.—The purpose of the Office shall be to protect against the unauthorized importation, possession, storage, transportation, development, or use of a nuclear explosive device, fissile material, or radiological material against the United States.

"(c) DIRECTOR.—The Office shall be headed by a Director of Domestic Nuclear Detection, who shall be appointed by the President from among individuals nominated by the Secretary. No individual shall be appointed Director of Domestic Nuclear Detection unless the individual has by education or experience demonstrated knowledge, ability, and skill in a field applicable to the detection and prevention of nuclear or radiological terrorism.

"(d) LIMITATION.—This title shall not be construed to affect the performance, by directorates and agencies of the Department other than the Office, of functions that are not related to detection and prevention of nuclear and radiological terrorism.

"SEC. 1902. RESPONSIBILITIES OF DIRECTOR OF DOMESTIC NUCLEAR DETECTION.

"(a) IN GENERAL.—The Secretary shall vest in the Director of Domestic Nuclear Detection the primary responsibility in the Department for—

"(1) administering all nuclear and radiological detection and prevention functions and assets of the Department; and

"(2) for coordinating such administration with nuclear and radiological detection and prevention activities of other Federal departments and agencies.

"(b) TRANSFER OF FUNCTIONS.—The Secretary shall transfer to the Director the authority to administer, or supervise the administration of, all functions, personnel, assets, and liabilities of all Department programs and projects relating to nuclear and radiological detection research, development, testing, and evaluation, and nuclear and radiological detection system acquisition and deployment, including with respect to functions and assets transferred by section 303(1)(B), (C), and (E) and functions, assets, and personnel transferred pursuant to section 1910(c).

"SEC. 1903. GLOBAL NUCLEAR DETECTION ARCHITECTURE.

"(a) IN GENERAL.—The Director of Domestic Nuclear Detection shall coordinate the Federal Government's implementation of a global nuclear detection architecture.

"(b) FUNCTIONS OF DIRECTOR.—In carrying out subsection (a), the Director shall—

"(1) design a strategy that will guide deployment of the global nuclear detection architecture;

"(2) implement the strategy in the United States; and

"(3) coordinate Department and Federal interagency efforts to deploy the elements of the global nuclear detection architecture outside the United States.

"(c) RELATIONSHIP TO OTHER DEPARTMENTS AND AGENCIES.—The authority of the Director under this section shall not affect an authority or responsibility of any other department or agency of the Federal Government with respect to the deployment of nuclear and radiological detection systems outside the United States under any program administered by that department or agency.

"SEC. 1904. RESEARCH AND DEVELOPMENT.

"(a) IN GENERAL.—The Director of Domestic Nuclear Detection shall carry out a research and development program to achieve transformational and evolutionary improvements in detection capabilities for shielded and unshielded nuclear explosive devices and radiological dispersion devices.

"(b) HIGH-RISK PROJECTS.—The program shall include funding for transformational research and development projects that may have a high risk of failure but have the potential to provide significant benefits.

"(c) LONG-TERM PROJECTS.—In order to reflect a long-term commitment to the development of more effective detection technologies, the program shall include the provision of funding for projects having a duration of more than 3 years, as appropriate.

"(d) COORDINATION WITH OTHER FEDERAL PROGRAMS.—The Director shall coordinate implementation of the program with other Federal agencies performing similar research and development in order to accelerate the development of effective technologies, promote technology sharing, and to avoid duplication, including through the use of the interagency coordination council established under section 1913.

"SEC. 1905. SYSTEM ASSESSMENTS.

"(a) PROGRAM REQUIRED.—The Director of Domestic Nuclear Detection shall carry out a program to test and evaluate technology for detecting nuclear explosive devices and fissile or radiological material.

"(b) PERFORMANCE METRICS.—The Director shall establish performance metrics for evaluating the effectiveness of individual detectors and detection systems in detecting nuclear explosive devices or fissile or radiological material—

"(1) under realistic operational and environmental conditions; and

"(2) against realistic adversary tactics and countermeasures.

"(c) PROVISION OF TESTING SERVICES.—

"(1) IN GENERAL.—The Director may, under the program required under subsection (a), make available testing services to developers of detection technologies. The results of the tests performed with services made available under this subsection shall be confidential and may not be disclosed to individuals or entities outside of the Federal Government without the consent of the developer for whom the tests are performed.

"(2) FEES.—The Director may charge a fee, as appropriate, to perform any service under this subsection.

"(d) SYSTEM ASSESSMENTS.—

"(1) IN GENERAL.—The Director shall periodically perform system-wide assessments of the global nuclear detection architecture to identify vulnerabilities and to gauge overall system performance against nuclear and radiological threats.

"(2) INCLUDED ACTIVITIES.—The assessments shall include—

"(A) red teaming activities to identify vulnerabilities and possible modes of attack and concealment methods; and

"(B) net assessments to determine architecture performance against adversary tactics and concealment methods.

"(3) USE.—The Director shall use the assessments to guide deployment of the global nuclear detection architecture and the research and development activities of the Office of Domestic Nuclear Detection.

"SEC. 1906. TECHNOLOGY ACQUISITION, DEPLOYMENT, SUPPORT, AND TRAINING.

"(a) ACQUISITION STRATEGY.—

"(1) IN GENERAL.—The Director of Domestic Nuclear Detection shall develop and, subject to the availability of appropriations, execute a strategy for the acquisition and deployment of detection systems in order to implement the Department components of the global nuclear detection architecture developed under section 1903.

"(2) USE OF AVAILABLE CONTRACTING PROCEDURES.—The Director shall make use of all contracting procedures available to the Secretary to implement the acquisition strategy.

"(3) DETERMINATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGY.—The Director shall make recommendations based on the criteria included in section 862(b) as to whether the detection systems acquired pursuant to this subsection shall be designated by the Secretary as anti-terrorism technologies that qualify for protection under the system of risk management under subtitle G of title VIII. The Under Secretary for Science and Technology shall consider the Director's recommendations and expedite the process of determining whether such detection systems shall be designated as anti-terrorism technologies that qualify for such protection.

"(b) DEPLOYMENT.—The Director shall deploy detection systems for use by Department operational units and other end-users in implementing the global nuclear detection architecture.

"(c) OPERATIONAL SUPPORT AND PROTOCOLS.—

"(1) OPERATIONAL SUPPORT.—The Director shall provide operational support for all systems acquired to implement the acquisition strategy developed under subsection (a).

"(2) OPERATIONAL PROTOCOLS.—The Director shall develop operational protocols for detection technology acquired and deployed to implement the acquisition strategy, including procedures for alarm resolution and notification of appropriate response agencies in the event that illicit nuclear, radioactive, or fissile materials are detected by such a product or service.

"(3) TECHNICAL REACHBACK.—The Director will ensure that the expertise necessary to accurately interpret detection data is made available in a timely manner for all technology deployed to implement the global nuclear detection architecture.

"(d) TRAINING.—The Director shall develop and distribute training materials and provide training to all end-users of technology acquired by the Director under the acquisition strategy.

"(e) SOLICITATION OF END-USER INPUT.—In developing requirements for the research and development program of section 1904 and requirements for the acquisition of detection systems to implement the strategy in subsection (a), the Director shall solicit input from end-users of such systems.

"(f) STATE AND LOCAL SUPPORT.—Upon request, the Director shall provide guidance regarding radiation detection technology acquisitions to be made by State, local, and tribal governments and emergency response providers.

"SEC. 1907. SITUATIONAL AWARENESS.

"(a) DETECTION INFORMATION.—The Director of Domestic Nuclear Detection—

"(1) shall continuously monitor detection information received from foreign and domestic detection systems to maintain for the Department a situational awareness of all nuclear threats; and

"(2) shall gather and archive—

"(A) detection data measurements taken of benign activities in the normal flows of commerce; and

"(B) alarm data, including false alarms and nuisance alarms.

"(b) INFORMATION SHARING.—The Director shall coordinate with other governmental agencies to ensure that the detection of unauthorized nuclear explosive devices, fissile material, or radiological material is promptly reported to all appropriate Federal response agencies including the Attorney General, the Director of the Federal Bureau of Investigation, the Secretary of Defense, and the Secretary of Energy.

"(c) INCIDENT RESOLUTION.—The Director shall assess nuclear threats communicated by Federal, State, tribal, or local officials and provide adequate technical reachback capability for swift and effective incident resolution.

"(d) SECURITY.—The Director shall—

"(1) develop and implement security standards and protocols for the control and protection of all classified or sensitive information in possession of the Office; and

"(2) ensure that relevant personnel of the Office have the required security clearances to properly handle such information.

"SEC. 1908. FORENSIC ANALYSIS.

"The Director of Domestic Nuclear Detection shall perform all research, development, and acquisition activities of the Department pertaining to forensic analysis and attribution of nuclear and radiological attacks.

"SEC. 1909. THREAT INFORMATION.

"(a) THREAT ASSESSMENTS.—The Director of Domestic Nuclear Detection shall utilize classified and unclassified nuclear and radiological threat assessments in designing the global nuclear detection architecture under section 1903, prioritizing detection system deployments, and testing and optimizing system performance of that architecture, including assessments of—

"(1) smuggling routes;

"(2) locations of relevant nuclear and radiological material throughout the world;

"(3) relevant terrorist tradecraft and concealment methods; and

"(4) relevant nuclear and radiological threat objects in terms of possible detection signatures.

"(b) ACCESS TO INFORMATION.—The Secretary shall provide the Director access to all information relating to nuclear and radiological threats, including reports, assessments, analyses, and unevaluated intelligence, that is necessary to successfully design, deploy, and support the operation of an effective global detection architecture under section 1903.

"(c) ANALYTICAL SUPPORT.—The Director shall request that the Secretary provide to the Director, pursuant to section 201(c)(20), the requisite intelligence and infor-

mation analysis support necessary to effectively discharge the Director's responsibilities.

"(d) ANALYTICAL EXPERTISE.—For the purposes of performing any of the assessments required under subsection (a), the Director, subject to the availability of appropriations, may hire qualified personnel with experience in performing nuclear and radiological threat assessments.

"(e) COLLECTION REQUESTS.—The Director shall recommend that the Secretary consult with the Director of Central Intelligence or other appropriate intelligence, law enforcement, or other elements of the Federal Government pursuant to section 201(c)(7) with respect to intelligence collection to design, deploy, and support the operation of the global detection architecture under section 1903.

"SEC. 1910. ADMINISTRATIVE AUTHORITIES.

"(a) HIRING.—In hiring personnel for the Office of Domestic Nuclear Detection, the Secretary shall have the hiring and management authorities described in section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note; Public Law 105–261). The term of appointments for employees under subsection (c)(1) of that section may not exceed 5 years before the granting of any extension under subsection (c)(2) of that section

"(b) DETAIL OF PERSONNEL.—In order to assist the Director of Domestic Nuclear Detection in discharging the Director's responsibilities, personnel of other Federal agencies may be detailed to the Office for the performance of analytic functions and related duties.

"(c) TRANSFER OF SCIENCE AND TECHNOLOGY FUNCTIONS, PERSONNEL, AND ASSETS.—

"(1) TRANSFER REQUIRED.—Except as provided in paragraph (2), the Secretary shall transfer to the Director the functions, assets, and personnel of the Department relating to radiological and nuclear countermeasures, including forensics of contaminated evidence and attack attribution.

"(2) EXCEPTIONS.—The Secretary shall not transfer under paragraph (1) functions, assets, and personnel relating to consequence management and recovery.

"(3) ELIMINATION OF DUPLICATION OF EFFORT.—The Secretary shall ensure that to the extent that complementary functions are vested in the Directorate of Science and Technology and the Office of Domestic Nuclear Detection with respect to radiological and nuclear countermeasures, the Under Secretary for Science and Technology and the Director of Domestic Nuclear Detection coordinate the programs administered by the Under Secretary and the Director to eliminate duplication and increase integration opportunities, particularly with respect to technology development and test and evaluation.

"SEC. 1911. REPORT REQUIREMENT.

"The Director of Domestic Nuclear Detection shall submit to Congress an annual report on each of the following:

"(1) The global detection strategy developed under section 1903.

"(2) The status of implementation of such architecture.

"(3) The schedule for future detection system deployments under such architecture.

"(4) The research and development program of the Office of Domestic Nuclear Detection.

"(5) A summary of actions taken by the Office during the reporting period to counter nuclear and radiological threats.

"SEC. 1912. ADVISORY COUNCIL ON NUCLEAR DETECTION.

"(a) ESTABLISHMENT.—Pursuant to section 871 of this Act, the Secretary shall establish within the Office of Domestic Nuclear Detection an Advisory Council on Nuclear Detection (in this section referred to as the 'Advisory Council'). The Advisory Council shall report to the Director of Domestic Nuclear Detection.

"(b) FUNCTIONS.—The Advisory Council shall, at the request of the Director—

"(1) advise the Director on recommendations for the global nuclear detection architecture developed under section 1903(a);

"(2) identify research areas for development of next-generation and transformational nuclear and radiological detection technologies; and

"(3) and have such additional responsibilities as the Director may assign in furtherance of the Department's homeland security mission with respect to enhancing domestic and international nuclear and radiological detection capabilities.

"(c) MEMBERSHIP.—The Advisory Council shall consist of 5 members appointed by the Director, who shall—

"(1) be individuals who have an eminent knowledge and technical expertise related to nuclear and radiological detection research and development and radiation detection;

"(2) be selected solely on the basis of their established record of distinguished service; and

"(3) not be employees of the Federal Government, other than employees of National Laboratories.

"(d) CONFLICT OF INTEREST RULES.—The Advisory Council shall establish rules for determining when one of its members has a conflict of interest in a matter being considered by the Advisory Council, and the appropriate course of action to address such conflicts of interest.

"SEC. 1913. INTERAGENCY COORDINATION COUNCIL.

"The President—

"(1) shall establish an interagency coordination council to facilitate interagency cooperation for purposes of implementing this title;

"(2) shall appoint the Secretary to chair the interagency coordination council; and

"(3) may appoint the Attorney General, the Secretary of Energy, the Secretary of State, the Secretary of Defense, and the heads of other appropriate Federal agencies to designate members to serve on such council.

"SEC. 1914. AUTHORIZATION OF APPROPRIATIONS.

"There is authorized to be appropriated to carry out this title—

"(1) from the amount authorized to be appropriated for fiscal year 2007 under section 101 of the Department of Homeland Security Authorization Act for Fiscal Year 2007, $536,000,000 for that fiscal year; and

"(2) such sums as may be necessary for each subsequent fiscal year.

"SEC. 1915. DEFINITIONS.

"In this title:

"(1) The term 'fissile materials' means material capable of undergoing nuclear fission by thermal or slow neutrons.

"(2) The term 'global nuclear detection architecture' means a multi-layered system of detectors deployed internationally and domestically to detect and interdict nuclear and radiological materials intended for illicit use.

"(3) The term 'nuclear and radiological detection system' means any technology that is capable of detecting or identifying nuclear and radiological material or explosive devices.

"(4) The term 'radiological material' means material that emits nuclear radiation.

"(5) The term 'nuclear explosive device' means an explosive device capable of producing a nuclear yield.

"(6) The term 'technical reachback' means technical expert support provided to operational end users for data interpretation and alarm resolution.

"(7) The term 'transformational' means that, if successful, will produce dramatic technological improvements over existing capabilities in the areas of performance, cost, or ease of use.".

(b) CONFORMING AMENDMENTS.—

(1) Section 103(d) of the Homeland Security Act of 2002 (6 U.S.C. 113(d)) is amended by adding at the end the following:

"(5) A Director of the Domestic Nuclear Detection Office.".

(2) Section 302 of such Act (6 U.S.C. 182) is amended—

(A) in paragraph (2) by striking ", radiological, nuclear"; and

(B) in paragraph (5)(A) by striking ", radiological, nuclear".

(3) Section 305 of such Act (6 U.S.C. 185) is amended by inserting "and the Director of the Domestic Nuclear Detection Office" after "Technology".

(4) Section 308 of such Act (6 U.S.C. 188) is amended in each of subsections (a) and (b)(1) by inserting "and the Director of the Domestic Nuclear Detection Office" after "Technology" each place it appears.

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (116 Stat. 2135) is amended by adding at the end the following:

"TITLE XIX—DOMESTIC NUCLEAR DETECTION

"Sec. 1901. Office of Domestic Nuclear Detection.
"Sec. 1902. Responsibilities of Director of Domestic Nuclear Detection.
"Sec. 1903. Global nuclear detection architecture.
"Sec. 1904. Research and development.
"Sec. 1905. System assessments.
"Sec. 1906. Technology acquisition, deployment, support, and training.
"Sec. 1907. Situational awareness.
"Sec. 1908. Forensic analysis.

"Sec. 1909. Threat information.
"Sec. 1910. Administrative authorities.
"Sec. 1911. Report requirement.
"Sec. 1912. Advisory Council on Nuclear Detection.
"Sec. 1913. Interagency coordination council.
"Sec. 1914. Authorization of appropriations.
"Sec. 1915. Definitions.".

SEC. 602. CHIEF MEDICAL OFFICER.

(a) ESTABLISHMENT.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.) is amended by adding at the end the following:

"SEC. 513. CHIEF MEDICAL OFFICER.

"(a) IN GENERAL.—There is in the Department a Chief Medical Officer, who shall be appointed by the President, by and with the advice and consent of the Senate.

"(b) QUALIFICATIONS.—The individual appointed as Chief Medical Officer shall possess a demonstrated ability in and knowledge of medicine and public health.

"(c) RESPONSIBILITIES.—The Chief Medical Officer shall have the primary responsibility within the Department for medical issues related to acts of terrorism, natural disasters, and other emergencies, including the following:

"(1) Serving as the Secretary's principal advisor on medical and public health issues.

"(2) Coordinating the biosurveillance and detection activities of the Department.

"(3) Ensuring that decision support tools link biosurveillance and detection information to near real-time response actions at the State, local, and tribal level.

"(4) Ensuring internal and external coordination of all medical preparedness and response activities of the Department, including training, exercises, and equipment support.

"(5) Serving as the Department's primary point of contact on medical and public health issues with the Departments of Agriculture, Defense, Health and Human Services, Transportation, and Veterans Affairs, and other Federal departments or agencies.

"(6) Serving as the Department's primary point of contact with respect to medical and public health matters.

"(7) Discharging, in coordination with the Under Secretary for Science and Technology, responsibilities of the Department related to Project Bioshield.

"(8) Establishing doctrine and priorities for the National Disaster Medical System and supervising its medical components, consistent with the National Response Plan and the National Incident Management System.

"(9) Establishing doctrine and priorities for the Metropolitan Medical Response System, consistent with the National Response Plan and the National Incident Management System.

"(10) Assessing the capability of the Department to contribute to enhancing the national medical surge capacity to respond to acts of terrorism, natural disasters, and other emergencies.

"(11) Performing such other duties relating to such responsibilities as the Secretary may require.

"(d) DEPUTY.—There is in the Department a Deputy Chief Medical Officer, who shall be appointed by the Secretary and who shall assist the Chief Medical Officer in carrying out the responsibilities under subsection (c).".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the item relating to section 512 (as added by section 307(a)) the following new item:

"Sec. 513. Chief Medical Officer.".

SEC. 603. NATIONAL BIOSURVEILLANCE INTEGRATION SYSTEM.

(a) ESTABLISHMENT.—The Secretary of Homeland Security, acting through the Chief Medical Officer of the Department of Homeland Security, shall establish a National Biosurveillance Integration System (referred to in this section as the "NBIS") to enhance the capability of the Federal Government to rapidly identify, characterize, and localize a biological event by integrating and analyzing data from human health, animal, plant, food, and environmental monitoring systems (both national and international) into a single comprehensive system.

(b) REQUIREMENTS.—The NBIS shall be designed to detect, as early as possible, a biological event that presents a risk to the United States or the infrastructure or key assets of the United States. The NBIS shall—

(1) consolidate data from all relevant surveillance systems maintained by the Department of Homeland Security and other governmental and private sources, both foreign and domestic;

(2) use an information technology system that uses the best available statistical and other analytical tools to automatically identify and characterize biological events in as close to real-time as possible; and

(3) process and protect sensitive data consistent with requirements of applicable privacy laws including the Health Insurance Portability and Accountability Act of 1996.

(c) RESPONSIBILITIES OF THE CHIEF MEDICAL OFFICER OF THE DEPARTMENT OF HOMELAND SECURITY.—

(1) IN GENERAL.—The Chief Medical Officer of the Department of Homeland Security shall—

(A) establish an entity to perform all operations and assessments related to the NBIS;

(B) continuously monitor the availability and appropriateness of data feeds and solicit new surveillance systems with data that would enhance biological situational awareness or overall NBIS performance;

(C) continuously review and seek to improve the statistical and other analytical methods utilized by NBIS;

(D) establish a procedure to enable States and local government entities to report suspicious events that could warrant further assessments using NBIS;

(E) receive and consider all relevant homeland security information; and

(F) provide technical assistance, as appropriate, to all Federal, regional, State, and local government entities and private sector entities that contribute data relevant to the operation of NBIS.

(2) ASSESSMENTS.—The Chief Medical Officer of the Department of Homeland Security shall—

(A) continuously evaluate available data for evidence of a biological event; and

(B) integrate homeland security information with NBIS data to provide overall situational awareness and determine whether a biological event has occurred.

(3) INFORMATION SHARING.—The Chief Medical Officer of the Department of Homeland Security shall—

(A) in the event that a biological event is detected, notify the Secretary of Homeland Security and disseminate results of NBIS assessments related to that biological event to appropriate Federal, regional, State, and local response entities in a timely manner to support decision making;

(B) provide reports on NBIS assessments to Federal, regional, State, and local governments and any private sector entities, as considered appropriate by the Secretary; and

(C) use available information sharing networks internal to the Department, as well as those within the intelligence community and operation centers, for distributing NBIS incident or situational awareness reports.

(d) NOTIFICATION OF CHIEF MEDICAL OFFICER OF THE DEPARTMENT OF HOMELAND SECURITY.—The Secretary of Homeland Security shall ensure that the Chief Medical Officer of the Department of Homeland Security is notified of any threat of a biological event and receives all classified and unclassified reports related to threats of biological events in a timely manner.

(e) ADMINISTRATIVE AUTHORITIES.—

(1) HIRING OF EXPERTS.—The Chief Medical Officer of the Department of Homeland Security shall hire individuals with the necessary expertise to develop and operate the NBIS system.

(2) DETAIL OF PERSONNEL.—Upon the request of the Chief Medical Officer of the Department of Homeland Security, the head of any Federal department or agency may detail, on a reimbursable basis, any of the personnel of that department or agency to the Department to assist the Chief Medical Officer of the Department of Homeland Security in carrying out this section.

(3) PRIVACY.—The Chief Medical Officer of the Department of Homeland Security shall ensure all applicable privacy regulations are strictly adhered to in the operation of the NBIS and the sharing of any information related to the NBIS.

(f) JOINT BIOSURVEILLANCE LEADERSHIP COUNCIL.—The Chief Medical Officer of the Department of Homeland Security shall—

(1) establish an interagency coordination council to facilitate interagency cooperation to advise the Chief Medical Officer of the Department of Homeland Security on recommendations to enhance the biosurveillance capabilities of the Department; and

(2) invite officials of Federal agencies that conduct biosurveillance programs, including the Department of Health and Human Services, the Department of

Agriculture, the Environment Protection Agency, and the Department of Defense, to serve on such council.

(g) ANNUAL REPORT REQUIRED.—Not later than December 31 of each year, the Chief Medical Officer of the Department of Homeland Security shall submit to Congress a report that contains each of the following:

(1) A list of departments, agencies, and private or nonprofit entities participating in the NBIS and the data each entity contributes to the NBIS.

(2) An implementation plan for the NBIS that includes cost, schedule, and key milestones.

(3) The status of the implementation of the NBIS.

(4) The schedule for obtaining access to any relevant biosurveillance information not compiled in NBIS as of the date on which the report is submitted.

(5) A description of the incident reporting or decision making protocols in effect as of the date on which the report is submitted and any changes made to such protocols during the period beginning on the date on which the report for the preceding year was submitted and ending on the date on which the report is submitted.

(6) A list of any Federal, State, or local government entities that have direct or indirect access to the information that is integrated into the NBIS.

(h) RELATIONSHIP TO OTHER DEPARTMENTS AND AGENCIES.—The authority of the Chief Medical Officer of the Department of Homeland Security under this section shall not affect an authority or responsibility of any other department or agency of the Federal Government with respect to biosurveillance activities under any program administered by that department or agency.

(i) BIOLOGICAL EVENT.—For purposes of this section, the term "biological event" means—

(1) an act of terrorism that uses material of biological origins; or

(2) a naturally occurring outbreak of an infectious disease that may affect national security.

SEC. 604. MATERIAL THREATS.

(a) IN GENERAL.—Section 319F–2(c)(2)(A) of the Public Health Service Act (42 U.S.C. 247d–6b(c)(2)(A)) is amended—

(1) by redesignating clauses (i) and (ii) as subclauses (I) and (II), respectively;

(2) by moving each of such subclauses two ems to the right;

(3) by striking "(A) MATERIAL THREAT.—The Homeland Security Secretary" and inserting the following:

"(A) MATERIAL THREAT.—

"(i) IN GENERAL.—The Homeland Security Secretary"; and

(4) by adding at the end the following clauses:

"(ii) USE OF EXISTING RISK ASSESSMENTS.—For the purpose of satisfying the requirements of clause (i) as expeditiously as possible, the Homeland Security Secretary shall, as practicable, utilize existing risk assessments that such Secretary considers credible.

"(iii) ORDER OF ASSESSMENTS.—

"(I) GROUPINGS TO FACILITATE ASSESSMENT OF COUNTERMEASURES.—In conducting threat assessments and determinations under clause (i) of chemical, biological, radiological, and nuclear agents, the Homeland Security Secretary shall, to the extent practicable and appropriate, consider the completion of such assessments and determinations for groups of agents toward the goal of facilitating the assessment of countermeasures under paragraph (3) by the Secretary of Health and Human Services.

"(II) CATEGORIES OF COUNTERMEASURES.—The grouping of agents under subclause (I) by the Homeland Security Secretary shall be designed to facilitate assessments under paragraph (3) by the Secretary of Health and Human Services regarding the following two categories of countermeasures:

"(aa) Countermeasures that may address more than one agent identified under clause (i)(II).

"(bb) Countermeasures that may address adverse health consequences that are common to exposure to different agents.

"(III) RULE OF CONSTRUCTION.—A particular grouping of agents pursuant to subclause (II) is not required under such subclause to facilitate assessments of both categories of countermeasures described in such subclause. A grouping may concern one category and not the other.

"(iv) TIME FRAME FOR COMPLETION OF CERTAIN NATIONAL-SECURITY DETERMINATIONS.—With respect to chemical, biological, radiological,

and nuclear agents known to the Homeland Security Secretary as of the day before the date of the enactment of this Act, and which such Secretary considers to be capable of significantly affecting national security, such Secretary shall complete the determinations under clause (i)(II) not later than December 31, 2007.

"(v) DEFINITION.—For purposes of this subparagraph, the term 'risk assessment' means a scientific, technically-based analysis of agents that incorporates threat, vulnerability, and consequence information.".

(b) AUTHORIZATION OF APPROPRIATIONS.—Section 510(d) of the Homeland Security Act of 2002 (6 U.S.C. 320(d)) is amended—

(1) in paragraph (1), by striking "2006," and inserting "2009,"; and

(2) by adding at the end the following:

"(3) ADDITIONAL AUTHORIZATION OF APPROPRIATIONS REGARDING CERTAIN THREAT ASSESSMENTS.—For the purpose of providing an additional amount to the Secretary to assist the Secretary in meeting the requirements of clause (iv) of section 319F–2(c)(2)(A)) of the Public Health Service Act (relating to time frames), there are authorized to be appropriated such sums as may be necessary for fiscal year 2007, in addition to the authorization of appropriations established in paragraph (1). The purposes for which such additional amount may be expended include conducting risk assessments regarding clause (i)(II) of such section when there are no existing risk assessments that the Secretary considers credible.".

SEC. 605. STUDY ON NATIONAL BIODEFENSE TRAINING.

(a) STUDY REQUIRED.—The Secretary of Homeland Security shall, in consultation with the Secretary of Defense and the Secretary for Health and Human Services, conduct a study to determine the staffing and training requirements for pending capital programs to construct biodefense laboratories (including agriculture and animal laboratories) at Biosafety Level 3 and Biosafety Level 4 or to expand current biodefense laboratories to such biosafety levels.

(b) ELEMENTS.—In conducting the study, the Secretary of Homeland Security shall address the following:

(1) The number of trained personnel, by discipline and qualification level, required for existing biodefense laboratories at Biosafety Level 3 and Biosafety Level 4.

(2) The number of research and support staff, including researchers, laboratory technicians, animal handlers, facility managers, facility or equipment maintainers, biosecurity personnel (including biosafety, physical, and electronic security personnel), and other safety personnel required to manage biodefense research efforts to combat bioterrorism at the biodefense laboratories described in subsection (a).

(3) The training required to provide the personnel described by paragraphs (1) and (2), including the type of training (whether classroom, laboratory, or field training) required, the length of training required by discipline, and the curriculum required to be developed for such training.

(4) Training schedules necessary to meet the scheduled openings of the biodefense laboratories described in subsection (a), including schedules for refresher training and continuing education that may be necessary for that purpose.

(c) REPORT.—Not later than December 31, 2006, the Secretary of Homeland Security shall submit to Congress a report setting forth the results of the study conducted under this section.

SEC. 606. HOMELAND SECURITY SCIENCE AND TECHNOLOGY ADVISORY COMMITTEE.

Section 311(j) of the Homeland Security Act of 2002 (6 U.S.C. 191(j)) is amended to read as follows:

"(j) TERMINATION.—The Department of Homeland Security Science and Technology Advisory Committee shall terminate on the date that is 10 years after the date on which it was established.".

TITLE VII—HOMELAND SECURITY INFRASTRUCTURE PROTECTION AND CYBERSECURITY ENHANCEMENT

SEC. 701. INFRASTRUCTURE PROTECTION AND CYBERSECURITY.

(a) IN GENERAL.—Title II of the Homeland Security Act of 2002 is amended by adding at the end the following new subtitle:

"Subtitle E—Infrastructure Protection and Cybersecurity

"SEC. 241. OFFICE OF INFRASTRUCTURE PROTECTION.

"(a) IN GENERAL.—There is in the Department an Office of Infrastructure Protection.

"(b) ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION.—The head of the Office shall be the Assistant Secretary for Infrastructure Protection.

"(c) RESPONSIBILITIES OF THE ASSISTANT SECRETARY.—The Assistant Secretary shall carry out the responsibilities of the Department regarding infrastructure protection. Such responsibilities shall include the following:

"(1) To identify and carry out comprehensive risk assessments of key resources and critical infrastructure of the United States, to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

"(2) To develop and maintain a comprehensive national plan for securing the key resources and critical infrastructure of the United States, in accordance with Homeland Security Presidential Directive 7.

"(3) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Departments and agencies and in consultation with State, local, and tribal government agencies and authorities, and the private sector.

"(4) To coordinate and implement, as appropriate, preparedness efforts to ensure that critical infrastructure and key resources efforts are fully integrated and coordinated with the response and recovery activities of the Department.

"(5) To establish and maintain partnerships and information sharing processes with Federal, State, local, and tribal governments, the private sector, and international governments and organizations to enhance coordination of critical infrastructure and key resource efforts.

"(6) To coordinate with the Under Secretary for Intelligence and Analysis and elements of the intelligence community and with Federal, State, local, and tribal law enforcement agencies, and the private sector, as appropriate.

"(7) To provide the Secretary with an annual summary of national critical infrastructure protection efforts and priorities and to provide, in consultation with the appropriate Department official with primary responsibility for grants, recommendations for Federal critical infrastructure protection funding.

"(8) In carrying out responsibilities under paragraphs (1) and (2), to consult with other Federal, State, local, and tribal government agencies and authorities as appropriate.

"(9) To perform other such duties relating to such responsibilities as the Secretary may provide.

"(d) INTEGRATION CENTER.—

"(1) IN GENERAL.—There is an Integration Center in the Office of Infrastructure Protection, which shall be staffed by the Office of Infrastructure Protection, the Office of Cybersecurity and Telecommunications, and the Office of Intelligence and Analysis.

"(2) RESPONSIBILITIES.—The Integration Center shall—

"(A) be responsible for the integration of relevant threat, consequence, and vulnerability information, analysis, and assessments (whether such information, analysis, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other Federal departments and agencies, State, local, and tribal government agencies and authorities, the private sector, and other entities; and

"(B) develop and disseminate analytical products that combine homeland security information with critical infrastructure and key resource vulnerability and consequence information.

"(3) CRITICAL INFRASTRUCTURE INFORMATION.—The Secretary shall ensure that the Department makes full and efficient use of open-source information to analyze United States critical infrastructure from the perspective of terrorists using publicly available information.

"(e) STAFF.—

"(1) IN GENERAL.—The Secretary shall ensure that the Office has staff that possess appropriate expertise and experience to assist the Assistant Secretary in discharging responsibilities under this section.

"(2) PRIVATE SECTOR STAFF.—Staff under this subsection may include individuals from the private sector.

"(3) SECURITY CLEARANCES.—Staff under this subsection shall possess security clearances appropriate for their work under this section.

"(f) DETAIL OF PERSONNEL.—

"(1) IN GENERAL.—In order to assist the Office in discharging responsibilities under this section, personnel of other Federal departments and agencies may be detailed to the Department for the performance of analytic functions and related duties.

"(2) COOPERATIVE AGREEMENTS.—The Secretary and the head of the Federal department or agency concerned may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

"(3) BASIS.—The detail of personnel under this subsection may be on a reimbursable or non-reimbursable basis.

"(g) REPROGRAMMING.—The Secretary may not reprogram any funds allocated to the Office of Infrastructure Protection until 60 days after the Secretary submits to the Committees on Appropriations of the Senate and House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives written notification of the reprogramming.

"SEC. 242. OFFICE OF CYBERSECURITY AND TELECOMMUNICATIONS.

"(a) IN GENERAL.—There is in the Department an Office of Cybersecurity and Telecommunications.

"(b) ASSISTANT SECRETARY FOR CYBERSECURITY AND TELECOMMUNICATIONS.—The head of the Office shall be the Assistant Secretary for Cybersecurity and Telecommunications.

"(c) RESPONSIBILITIES OF THE ASSISTANT SECRETARY.—The Assistant Secretary shall carry out the responsibilities of the Department regarding cybersecurity and telecommunications. Such responsibilities shall include the following:

"(1) To establish and manage—

"(A) a national cybersecurity response system that includes the ability to—

"(i) analyze the effect of cybersecurity threat information on national critical infrastructure identified by the President; and

"(ii) aid in the detection and warning of potential vulnerabilities or attacks that could cause widespread disruption of cybersecurity infrastructure and in the restoration of such infrastructure in the aftermath of such attacks;

"(B) a national cybersecurity threat and vulnerability reduction program which conducts risk assessments on information technology systems, identifies and prioritize vulnerabilities in critical information infrastructure, and coordinates the mitigation of such vulnerabilities;

"(C) an emergency communications program to ensure communications systems and procedures are in place to exchange information during disasters;

"(D) a continuity of operations program to plan and allocate resources for the continuation of critical information operations in the event of a large scale disruption of the information infrastructure and to coordinate a response;

"(E) a reconstitution program to ensure that priorities, procedures, and resources are in place to reconstitute critical information infrastructures. This program should clearly delineate roles and responsibilities of the Department, other federal agencies and private sector;

"(F) a resiliency program that will support basic and fundamental research to improve the reliability and security of network protocols;

"(G) a national public-private cybersecurity awareness, training, and education program that promotes Internet security awareness among all enduser groups;

"(H) a government cybersecurity program to coordinate and consult with Federal, State, and local governments to enhance their cybersecurity programs; and

"(I) an international cybersecurity cooperation program to help foster Federal efforts to enhance international cybersecurity awareness and cooperation.

"(2) To coordinate and to leverage existing efforts within the private sector on the program under paragraph (1) as appropriate and to promote cybersecurity information sharing, vulnerability assessment, and threat warning regarding critical infrastructure.

"(3) To coordinate with the Under Secretary for Intelligence and Analysis and the Assistant Secretary for Infrastructure Protection to provide relevant and timely homeland security information to the appropriate private sector information infrastructure stakeholders regarding potential vulnerabilities or attacks.

"(4) To coordinate with other directorates and offices within the Department and with other Federal agencies, as appropriate, with respect to the cybersecurity aspects of such directorates, offices, and agencies.

"(5) To coordinate with the Department official with primary responsibility for emergency preparedness to ensure that the National Response Plan developed includes appropriate measures for the recovery of the cybersecurity elements of critical infrastructure.

"(6) To promote voluntary cybersecurity best practices, standards, and benchmarks that are responsive to rapid technology changes and to the security needs of critical infrastructure.

"(7) To coordinate with the Chief Information Officer of the Department in establishing a secure information sharing architecture and information sharing processes, including with respect to the Department's operation centers.

"(8) To consult with the Electronic Crimes Task Force of the United States Secret Service on private sector outreach and information activities.

"(9) To consult with the appropriate Department official with primary responsibility for grants to ensure that realistic cybersecurity scenarios are incorporated into training exercises, including tabletop and recovery exercises.

"(10) To consult and coordinate with the Assistant Secretary for Infrastructure Protection, the Under Secretary for Science and Technology, and, where appropriate, with other relevant Federal departments and agencies, as well as private sector stakeholders, on the security of digital control systems, such as Supervisory Control and Data Acquisition (SCADA) systems.

"(11) To consult and coordinate with the Under Secretary of Science and Technology on cybersecurity research and development requirements.

"(d) REPORTING.—Not later than one year after the date of the enactment of this section, the Secretary shall submit to Congress a report on the programs that implement or support the requirements of this section and the coordination of the Assistant Secretary with the private sector in meeting these responsibilities.

"(e) DEADLINE FOR NOMINATION.—Not later than 90 days after the date of the enactment of this section, the President shall nominate an individual to serve as the Assistant Secretary for Cybersecurity and Telecommunications.

"(f) STAFF.—

"(1) IN GENERAL.—The Secretary shall provide the Office of Cybersecurity and Telecommunications with a staff having appropriate expertise and experience to assist the Assistant Secretary in discharging responsibilities under this section.

"(2) SECURITY CLEARANCES.—Staff under this subsection shall possess security clearances appropriate for their work under this section.

"(g) DETAIL OF PERSONNEL.—

"(1) IN GENERAL.—In order to assist the Assistant Secretary for Cybersecurity and Telecommunications in discharging the responsibilities of the Assistant Secretary under this section, personnel of other Federal departments and agencies may be detailed to the Department for the performance of analytic functions and related duties.

"(2) COOPERATIVE AGREEMENTS.—The Secretary and the head of a Federal department or agency concerned may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

"(3) BASIS.—The detail of personnel under this subsection may be on a reimbursable or non-reimbursable basis.

"(h) REPROGRAMMING.—The Secretary may not reprogram any funds allocated to the Office of Cybersecurity and Telecommunications until 60 days after the Secretary submits to the Committees on Appropriations of the Senate and House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives written notification of the reprogramming.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the items relating to subtitle D of title II the following:

"Subtitle E—Infrastructure Protection and Cybersecurity

"Sec. 241. Office of Infrastructure Protection.
"Sec. 242. Office of Cybersecurity and Telecommunications.".

SEC. 702. CRITICAL INFRASTRUCTURE STUDY.

(a) REQUIREMENT.—The Secretary of Homeland Security shall conduct a study to—

(1) determine the extent to which architecture, engineering, surveying, and mapping activities related to the critical infrastructure of the United States are being sent to offshore locations;

(2) assess whether any vulnerabilities or threats exist; and

(3) recommend policies, regulations, or legislation, as appropriate, that may be necessary to protect the national and homeland security interests of the United States.

(b) CONSULTATION.—In carrying out the study authorized by this section, the Secretary shall consult with—

(1) such other agencies of the Government of the United States as are appropriate; and

(2) national organizations representing the architecture, engineering, surveying, and mapping professions.

(c) REPORT.—The Secretary shall submit to the Congress by not later than 6 months after the date of the enactment of this Act a report on the findings, conclusions, and recommendations of the study under this section.

(d) DEFINITIONS.—As used in this section—

(1) each of the terms "architectural", "engineering", "surveying", and "mapping"—

(A) subject to subparagraph (B), has the same meaning such term has under section 1102 of title 40, United States Code; and

(B) includes services performed by professionals such as surveyors, photogrammetrists, hydrographers, geodesists, or cartographers in the collection, storage, retrieval, or dissemination of graphical or digital data to depict natural or man-made physical features, phenomena, or boundaries of the earth and any information related to such data, including any such data that comprises the processing of a survey, map, chart, geographic information system, remotely sensed image or data, or aerial photograph; and

(2) the term "critical infrastructure"—

(A) means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters; and

(B) includes the basic facilities, structures, and installations needed for the functioning of a community or society, including transportation and communications systems, water and power lines, power plants, and the built environment of private and public institutions of the United States.

SEC. 703. CYBERSECURITY TRAINING PROGRAM AND EQUIPMENT.

(a) IN GENERAL.—The Secretary of Homeland Security, acting through the Assistant Secretary of Homeland Security for Cybersecurity and Telecommunications, may establish, in conjunction with the National Science Foundation, a program to award grants to institutions of higher education (and consortia thereof) for—

(1) the establishment or expansion of cybersecurity professional development programs;

(2) the establishment or expansion of associate degree programs in cybersecurity; and

(3) the purchase of equipment to provide training in cybersecurity for either professional development programs or degree programs.

(b) ROLES.—

(1) DEPARTMENT OF HOMELAND SECURITY.—The Secretary of Homeland Security, acting through the Assistant Secretary of Homeland Security for Cybersecurity and Telecommunications and in consultation with the Director of the National Science Foundation, shall establish the goals for the program established under this section and the criteria for awarding grants under the program.

(2) NATIONAL SCIENCE FOUNDATION.—The Director of the National Science Foundation shall operate the program established under this section consistent with the goals and criteria established under paragraph (1), including soliciting applicants, reviewing applications, and making and administering grant awards. The Director may consult with the Assistant Secretary for Cybersecurity and Telecommunications in selecting awardees.

(3) FUNDING.—The Secretary shall transfer to the National Science Foundation the funds necessary to carry out this section.

(c) GRANT AWARDS.—

(1) PEER REVIEW.—All grant awards under this section shall be made on a competitive, merit-reviewed basis.

(2) FOCUS.—In making grant awards under this section, the Director shall, to the extent practicable, ensure geographic diversity and the participation of women and underrepresented minorities.

(3) PREFERENCE.—In making grant awards under this section, the Director shall give preference to applications submitted by consortia of institutions to encourage as many students and professionals as possible to benefit from this program.

(d) AUTHORIZATION OF APPROPRIATIONS.—Of the amount authorized to be appropriated under section 101 for fiscal year 2007, $3,700,000 is to carry out this section for that fiscal year.

(e) DEFINITION.—For purposes of this section, the term "institution of higher education" has the meaning given that term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

SEC. 704. NATIONAL ASSET DATABASE.

(a) USE OF THE NATIONAL ASSET DATABASE.—

(1) IN GENERAL.—The Secretary of Homeland Security shall seek to reduce the vulnerability of the United States to terrorism and deny the use of infrastructure as a weapon, by—

(A) maintaining a catalog of the Nation's most at risk infrastructure in a single repository of national assets known as the National Asset Database, and use such database in the development, coordination, integration, and implementation of plans and programs, including to identify, catalog, prioritize, and protect critical infrastructure and key resources in accordance with Homeland Security Presidential Directive number 7, and in cooperation with all levels of government and private sector entities that the Secretary considers appropriate; and

(B) consulting the National Asset Database, along with other appropriate resources, in providing any covered grant to assist in preventing, reducing, mitigating, or responding to terrorist attack.

(2) REPORTS.—

(A) IN GENERAL.—The Secretary shall annually report to the congressional homeland security committees on critical infrastructure included in the National Asset Database that is most at risk to terrorism.

(B) CONTENTS.—Each report shall include the following:

(i) The name, location, and sector classification of assets in the National Asset Database that have been identified or deemed critical infrastructure that is most at risk to terrorism.

(ii) Changes made in such database regarding such critical infrastructure made during the period covered by the report regarding—

(I) defining and identifying critical infrastructure; and

(II) compiling a usable database.

(iii) The extent to which the database has been used as a tool for allocating funds to prevent, reduce, mitigate, and respond to terrorist attacks.

(C) CLASSIFIED INFORMATION.—The Secretary shall provide a classified briefing to the members of the congressional homeland security committees. The Secretary shall also submit with each report a classified annex containing information required to be submitted under this subsection that cannot be made public.

(3) DEFINITIONS.—In this subsection:

(A) CONGRESSIONAL HOMELAND SECURITY COMMITTEES.—The term "congressional homeland security committees" means the Committee on Homeland Security of the House of Representatives and the and the Committee on Homeland Security and Governmental Affairs of the Senate.

(B) NATIONAL ASSET DATABASE.—The term "National Asset Database" means such database as defined and established under Homeland Security Presidential Directive number 7.

(C) COVERED GRANT.—The term "covered grant" means any grant provided by the Department of Homeland Security under any of the following:

(i) The Urban Area Security Initiative.

(ii) The Buffer Zone Protection Program.

(iii) Any other grant program administered by the Department, as determined appropriate by the Secretary.

(iv) Any successor to a program referred to in this paragraph.

(4) TERMINATION.—This subsection shall not apply after the end of the 4-year period beginning on the date of the enactment of this subsection.

(b) MANAGEMENT OF NATIONAL ASSET DATABASE.—

(1) MILESTONES AND GUIDELINES.—The Secretary of Homeland Security shall—

(A) identify and evaluate key milestones for the National Asset Database, including methods to integrate private sector assets and tasks that must be completed to eventually allocate homeland security grant programs based on the information contained in the database; and

(B) issue guidelines for—

(i) States to submit uniform information for possible inclusion in the National Asset Database; and

(ii) review of such submissions by the Department.

(2) ORGANIZATION OF INFORMATION IN DATABASE.—The Secretary shall—

(A) remove from the National Asset Database assets that are determined by the Secretary to be unverifiable and as not meeting national asset guidelines set forth by the Secretary in requests for information from States; and

(B) classify assets in the database according to the 17 sectors listed in National Infrastructure Protection Plan developed pursuant to Homeland Security Presidential Directive 7, ensuring that the assets in the National Asset Database can be categorized by State and locality, regionally, and in such a manner as is effective for grants and other purposes.

(3) MAINTENANCE OF DATABASE.—

(A) annually defining and systematically examining assets in the database that are described incorrectly or that do not meet national assets guidelines used by the Secretary to determine which assets should remain in the National Asset Database;

(B) annually providing a list to the States of assets referred to in subparagraph (A) for review before finalizing the decision of which assets to include in the National Asset Database;

(C) reviewing the guidelines to the States to ensure consistency and uniformity for inclusion and how the Department intends to use that data;

(D) meeting annually with the States to provide guidance and clarification of the guidelines to promote consistency and uniformity in submissions;

(E) utilizing on an ongoing basis the expert panels established by the Department to review and refine the National Asset Database; and

(F) utilizing the Department of Homeland Security's National Infrastructure Simulation and Analysis Center for the National Asset Database taxonomy and asset information in the National Asset Database and facilitating the future exchange of information between the National Asset Database and such center.

(c) DEADLINES.—

(1) FIRST REPORT REGARDING USE OF THE NATIONAL ASSET DATABASE.—The Secretary of Homeland Security shall submit the first report under subsection (a) by not later than 90 days after the date of the enactment of this Act.

(2) MANAGEMENT OF THE NATIONAL ASSET DATABASE.—The Secretary of Homeland Security shall—

(A) complete implementation of subsection (b)(1) by not later than 90 days after the date of the enactment of this Act; and

(B) complete implementation of subsection (b)(2) by not later than 1 year after the date of the enactment of this Act.

TITLE VIII—GRANTS ADMINISTRATION

SEC. 801. FASTER AND SMARTER FUNDING FOR FIRST RESPONDERS.

(a) IN GENERAL.—The Homeland Security Act of 2002 (Public Law 107–296; 6 U.S.C. 361 et seq.) is further amended—

(1) in section 1(b) in the table of contents by adding at the end the following:

"TITLE XX—FUNDING FOR FIRST RESPONDERS

"Sec. 2001. Definitions.
"Sec. 2002. Faster and Smarter Funding for First Responders.
"Sec. 2003. Covered grant eligibility and criteria.
"Sec. 2004. Risk-based evaluation and prioritization.
"Sec. 2005. Use of funds."; and

(2) by adding at the end the following:

"TITLE XX—FUNDING FOR FIRST RESPONDERS

"SEC. 2001. DEFINITIONS.

"In this title:

"(1) BOARD.—The term 'Board' means the First Responder Grants Board established under section 2004.

"(2) COVERED GRANT.—The term 'covered grant' means any grant to which this title applies under section 2002.

"(3) DIRECTLY ELIGIBLE TRIBE.—The term 'directly eligible tribe' means any Indian tribe or consortium of Indian tribes that—

"(A) meets the criteria for inclusion in the qualified applicant pool for Self-Governance that are set forth in section 402(c) of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 458bb(c));

"(B) employs at least 10 full-time personnel in a law enforcement or emergency response agency with the capacity to respond to calls for law enforcement or emergency services; and

"(C)(i) is located on, or within 5 miles of, an international border or waterway;

"(ii) is located within 5 miles of a facility designated as high-risk critical infrastructure by the Secretary;

"(iii) is located within or contiguous to one of the 50 largest metropolitan statistical areas in the United States; or

"(iv) has more than 1,000 square miles of Indian country, as that term is defined in section 1151 of title 18, United States Code.

"(4) ELEVATIONS IN THE THREAT ALERT LEVEL.—The term 'elevations in the threat alert level' means any designation (including those that are less than national in scope) that raises the homeland security threat level to either the highest or second highest threat level under the Homeland Security Advisory System referred to in section 201(d)(7).

"(5) EMERGENCY PREPAREDNESS.—The term 'emergency preparedness' shall have the same meaning that term has under section 602 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5195a).

"(6) ESSENTIAL CAPABILITIES.—The term 'essential capabilities' means the levels, availability, and competence of emergency personnel, planning, training, and equipment across a variety of disciplines needed to effectively and efficiently prevent, prepare for, respond to, and recover from acts of terrorism consistent with established practices.

"(7) FIRST RESPONDER.—The term 'first responder' shall have the same meaning as the term 'emergency response provider'.

"(8) INDIAN TRIBE.—The term 'Indian tribe' means any Indian tribe, band, nation, or other organized group or community, including any Alaskan Native village or regional or village corporation as defined in or established pursuant to the Alaskan Native Claims Settlement Act (43 U.S.C. 1601 et seq.), which is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians.

"(9) REGION.—The term 'region' means—

"(A) any geographic area consisting of all or parts of 2 or more contiguous States, counties, municipalities, or other local governments that have a combined population of at least 1,650,000 or have an area of not less than 20,000 square miles, and that, for purposes of an application for a covered grant, is represented by 1 or more governments or governmental agencies within such geographic area, and that is established by law or by agreement of 2 or more such governments or governmental agencies in a mutual aid agreement; or

"(B) any other combination of contiguous local government units (including such a combination established by law or agreement of two or more governments or governmental agencies in a mutual aid agreement) that is formally certified by the Secretary as a region for purposes of this Act with the consent of—

"(i) the State or States in which they are located, including a multi-State entity established by a compact between two or more States; and

"(ii) the incorporated municipalities, counties, and parishes that they encompass.

"(10) TERRORISM PREPAREDNESS.—The term 'terrorism preparedness' means any activity designed to improve the ability to prevent, prepare for, respond to, mitigate against, or recover from threatened or actual terrorist attacks.

"SEC. 2002. FASTER AND SMARTER FUNDING FOR FIRST RESPONDERS.

"(a) COVERED GRANTS.—This title applies to grants provided by the Department to States, regions, or directly eligible tribes for the primary purpose of improving the ability of first responders to prevent, prepare for, respond to, mitigate against, or recover from threatened or actual terrorist attacks, especially those involving weapons of mass destruction, administered under the following:

"(1) STATE HOMELAND SECURITY GRANT PROGRAM.—The State Homeland Security Grant Program of the Department, or any successor to such grant program.

"(2) URBAN AREA SECURITY INITIATIVE.—The Urban Area Security Initiative of the Department, or any successor to such grant program.

"(3) LAW ENFORCEMENT TERRORISM PREVENTION PROGRAM.—The Law Enforcement Terrorism Prevention Program of the Department, or any successor to such grant program.

"(b) EXCLUDED PROGRAMS.—This title does not apply to or otherwise affect the following Federal grant programs or any grant under such a program:

"(1) NONDEPARTMENT PROGRAMS.—Any Federal grant program that is not administered by the Department.

"(2) FIRE GRANT PROGRAMS.—The fire grant programs authorized by sections 33 and 34 of the Federal Fire Prevention and Control Act of 1974 (15 U.S.C. 2229, 2229a).

"(3) EMERGENCY MANAGEMENT PLANNING AND ASSISTANCE ACCOUNT GRANTS.—The Emergency Management Performance Grant program and the Urban Search and Rescue Grants program authorized by title VI of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5195 et seq.); the Departments of Veterans Affairs and Housing and Urban Development, and Independent Agencies Appropriations Act, 2000 (113 Stat. 1047 et seq.); and the Earthquake Hazards Reduction Act of 1977 (42 U.S.C. 7701 et seq.).

"SEC. 2003. COVERED GRANT ELIGIBILITY AND CRITERIA.

"(a) GRANT ELIGIBILITY.—Any State, region, or directly eligible tribe shall be eligible to apply for a covered grant.

"(b) GRANT CRITERIA.—The Secretary shall award covered grants to assist States and local governments in achieving, maintaining, and enhancing the essential capabilities for terrorism preparedness established by the Secretary.

"(c) STATE HOMELAND SECURITY PLANS.—

"(1) SUBMISSION OF PLANS.—The Secretary shall require that any State applying to the Secretary for a covered grant must submit to the Secretary a 3-year State homeland security plan that—

"(A) describes the essential capabilities that communities within the State should possess, or to which they should have access, based upon the terrorism risk factors relevant to such communities, in order to meet the Department's goals for terrorism preparedness;

"(B) demonstrates the extent to which the State has achieved the essential capabilities that apply to the State;

"(C) demonstrates the needs of the State necessary to achieve, maintain, or enhance the essential capabilities that apply to the State;

"(D) includes a prioritization of such needs based on threat, vulnerability, and consequence assessment factors applicable to the State;

"(E) describes how the State intends—

"(i) to address such needs at the city, county, regional, tribal, State, and interstate level, including a precise description of any regional structure the State has established for the purpose of organizing homeland security preparedness activities funded by covered grants;

"(ii) to use all Federal, State, and local resources available for the purpose of addressing such needs; and

"(iii) to give particular emphasis to regional planning and cooperation, including the activities of multijurisdictional planning agencies governed by local officials, both within its jurisdictional borders and with neighboring States;

"(F) with respect to the emergency preparedness of first responders, addresses the unique aspects of terrorism as part of a comprehensive State emergency management plan; and

"(G) provides for coordination of response and recovery efforts at the local level, including procedures for effective incident command in conformance with the National Incident Management System.

"(2) CONSULTATION.—The State plan submitted under paragraph (1) shall be developed in consultation with and subject to appropriate comment by local governments and first responders within the State.

"(3) APPROVAL BY SECRETARY.—The Secretary may not award any covered grant to a State unless the Secretary has approved the applicable State homeland security plan.

"(4) REVISIONS.—A State may revise the applicable State homeland security plan approved by the Secretary under this subsection, subject to approval of the revision by the Secretary.

"(d) CONSISTENCY WITH STATE PLANS.—The Secretary shall ensure that each covered grant is used to supplement and support, in a consistent and coordinated manner, the applicable State homeland security plan or plans.

"(e) APPLICATION FOR GRANT.—

"(1) IN GENERAL.—Except as otherwise provided in this subsection, any State, region, or directly eligible tribe may apply for a covered grant by submitting to the Secretary an application at such time, in such manner, and containing such information as is required under this subsection, or as the Secretary may reasonably require.

"(2) DEADLINES FOR APPLICATIONS AND AWARDS.—All applications for covered grants must be submitted at such time as the Secretary may reasonably require for the fiscal year for which they are submitted. The Secretary shall award covered grants pursuant to all approved applications for such fiscal year as soon as practicable, but not later than March 1 of such year.

"(3) AVAILABILITY OF FUNDS.—All funds awarded by the Secretary under covered grants in a fiscal year shall be available for obligation through the end of the subsequent fiscal year.

"(4) MINIMUM CONTENTS OF APPLICATION.—The Secretary shall require that each applicant include in its application, at a minimum—

"(A) the purpose for which the applicant seeks covered grant funds and the reasons why the applicant needs the covered grant to meet the essential capabilities for terrorism preparedness within the State, region, or directly eligible tribe to which the application pertains;

"(B) a description of how, by reference to the applicable State homeland security plan or plans under subsection (c), the allocation of grant funding proposed in the application, including, where applicable, the amount not passed through to local governments, first responders, and other local groups, would assist in fulfilling the essential capabilities for terrorism preparedness specified in such plan or plans;

"(C) a statement of whether a mutual aid agreement applies to the use of all or any portion of the covered grant funds;

"(D) if the applicant is a State, a description of how the State plans to allocate the covered grant funds to regions, local governments, and Indian tribes;

"(E) if the applicant is a region—

"(i) a precise geographical description of the region and a specification of all participating and nonparticipating local governments within the geographical area comprising that region;

"(ii) a specification of what governmental entity within the region will administer the expenditure of funds under the covered grant; and

"(iii) a designation of a specific individual to serve as regional liaison;

"(F) a capital budget showing how the applicant intends to allocate and expend the covered grant funds;

"(G) if the applicant is a directly eligible tribe, a designation of a specific individual to serve as the tribal liaison; and

"(H) a statement of how the applicant intends to meet the matching requirement, if any, that applies under section 2005(g).

"(5) REGIONAL APPLICATIONS.—

"(A) RELATIONSHIP TO STATE APPLICATIONS.—A regional application—

"(i) shall be coordinated with an application submitted by the State or States of which such region is a part;

"(ii) shall supplement and avoid duplication with such State application; and

"(iii) shall address the unique regional aspects of such region's terrorism preparedness needs beyond those provided for in the application of such State or States.

"(B) STATE REVIEW AND SUBMISSION.—To ensure the consistency required under subsection (d) and the coordination required under subparagraph (A), an applicant that is a region must submit its application to each State of which any part is included in the region for review and concurrence prior to the submission of such application to the Secretary. The regional application shall be transmitted to the Secretary through each such State within 30 days of its receipt, unless the Governor of such a State notifies the Sec-

retary, in writing, that such regional application is inconsistent with the State's homeland security plan and provides an explanation of the reasons therefor.

"(C) DISTRIBUTION OF REGIONAL AWARDS.—If the Secretary approves a regional application, then the Secretary shall distribute a regional award to the State or States submitting the applicable regional application under subparagraph (B), and each such State shall, not later than the end of the 45-day period beginning on the date after receiving a regional award, pass through to the region all covered grant funds or resources purchased with such funds, except those funds necessary for the State to carry out its responsibilities with respect to such regional application: *Provided*, That in no such case shall the State or States pass through to the region less than 80 percent of the regional award.

"(D) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS TO REGIONS.—Any State that receives a regional award under subparagraph (C) shall certify to the Secretary, by not later than 30 days after the expiration of the period described in subparagraph (C) with respect to the grant, that the State has made available to the region the required funds and resources in accordance with subparagraph (C).

"(E) DIRECT PAYMENTS TO REGIONS.—If any State fails to pass through a regional award to a region as required by subparagraph (C) within 45 days after receiving such award and does not request or receive an extension of such period, the region may petition the Secretary to receive directly the portion of the regional award that is required to be passed through to such region under subparagraph (C).

"(F) REGIONAL LIAISONS.—A regional liaison designated under paragraph (4)(E)(iii) shall—

"(i) coordinate with Federal, State, local, regional, and private officials within the region concerning terrorism preparedness;

"(ii) develop a process for receiving input from Federal, State, local, regional, and private sector officials within the region to assist in the development of the regional application and to improve the region's access to covered grants; and

"(iii) administer, in consultation with State, local, regional, and private officials within the region, covered grants awarded to the region.

"(6) TRIBAL APPLICATIONS.—

"(A) SUBMISSION TO THE STATE OR STATES.—To ensure the consistency required under subsection (d), an applicant that is a directly eligible tribe must submit its application to each State within the boundaries of which any part of such tribe is located for direct submission to the Department along with the application of such State or States.

"(B) OPPORTUNITY FOR STATE COMMENT.—Before awarding any covered grant to a directly eligible tribe, the Secretary shall provide an opportunity to each State within the boundaries of which any part of such tribe is located to comment to the Secretary on the consistency of the tribe's application with the State's homeland security plan. Any such comments shall be submitted to the Secretary concurrently with the submission of the State and tribal applications.

"(C) FINAL AUTHORITY.—The Secretary shall have final authority to determine the consistency of any application of a directly eligible tribe with the applicable State homeland security plan or plans, and to approve any application of such tribe. The Secretary shall notify each State within the boundaries of which any part of such tribe is located of the approval of an application by such tribe.

"(D) TRIBAL LIAISON.—A tribal liaison designated under paragraph (4)(G) shall—

"(i) coordinate with Federal, State, local, regional, and private officials concerning terrorism preparedness;

"(ii) develop a process for receiving input from Federal, State, local, regional, and private sector officials to assist in the development of the application of such tribe and to improve the tribe's access to covered grants; and

"(iii) administer, in consultation with State, local, regional, and private officials, covered grants awarded to such tribe.

"(E) LIMITATION ON THE NUMBER OF DIRECT GRANTS.—The Secretary may make covered grants directly to not more than 20 directly eligible tribes per fiscal year.

"(F) TRIBES NOT RECEIVING DIRECT GRANTS.—An Indian tribe that does not receive a grant directly under this section is eligible to receive funds

under a covered grant from the State or States within the boundaries of which any part of such tribe is located, consistent with the homeland security plan of the State as described in subsection (c). If a State fails to pass through funds, the tribe may petition the Secretary to receive payment in the same manner as a local government.

"(7) EQUIPMENT STANDARDS.—If an applicant for a covered grant proposes to upgrade or purchase, with assistance provided under the grant, new equipment or systems that do not meet or exceed any applicable national voluntary consensus standards, the applicant shall include in the application an explanation of why such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed such standards.

"SEC. 2004. RISK-BASED EVALUATION AND PRIORITIZATION.

"(a) FIRST RESPONDER GRANTS BOARD.—

"(1) ESTABLISHMENT OF BOARD.—The Secretary shall establish a First Responder Grants Board, consisting of—

"(A) the Secretary;

"(B) the Under Secretary for Science and Technology;

"(C) the Under Secretary for Policy;

"(D) the Director of the Federal Emergency Management Agency;

"(E) the Assistant Secretary for United States Immigration and Customs Enforcement;

"(F) the Chief Intelligence Officer;

"(G) the Administrator of the United States Fire Administration;

"(H) the Department official with primary responsibility for preparedness;

"(I) the Department official with primary responsibility for grants; and

"(J) the Administrator of the Animal and Plant Health Inspection Service.

"(2) CHAIRMAN.—

"(A) IN GENERAL.—The Secretary shall be the Chairman of the Board.

"(B) EXERCISE OF AUTHORITIES BY DEPUTY SECRETARY.—The Deputy Secretary of Homeland Security may exercise the authorities of the Chairman, if the Secretary so directs.

"(b) FUNCTIONS OF BOARD MEMBERS.—The Under Secretaries, Assistant Secretaries, Administrators, and other officials referred to in subsection (a)(1) shall seek to ensure that the relevant expertise and input of their staff are available to and considered by the Board.

"(c) PRIORITIZATION OF GRANT APPLICATIONS.—

"(1) FACTORS TO BE CONSIDERED.—The Board shall evaluate and annually prioritize all pending applications for covered grants based upon—

"(A) the degree to which they would, by achieving, maintaining, or enhancing the essential capabilities of the applicants on a nationwide basis, lessen the threat to, vulnerability of, and consequences for persons (including transient commuting and tourist populations) and critical infrastructure;

"(B) prior acts of international terrorism;

"(C) elevations in the threat alert level;

"(D) the existence of significant ports of entry; and

"(E) the most current risk assessment available of the threats of terrorism against the United States.

"(2) CRITICAL INFRASTRUCTURE SECTORS.—The Board specifically shall consider threats of terrorism against the following critical infrastructure sectors in all areas of the United States, urban and rural:

"(A) Agriculture and food.

"(B) Banking and finance.

"(C) Chemical industries.

"(D) The defense industrial base.

"(E) Emergency services.

"(F) Energy.

"(G) Government facilities.

"(H) Postal and shipping.

"(I) Public health and health care.

"(J) Information technology.

"(K) Telecommunications.

"(L) Transportation systems.

"(M) Water.

"(N) Dams.

"(O) Commercial facilities.

"(P) National monuments and icons.

"(Q) Commercial nuclear reactors, materials, and waste.

The order in which the critical infrastructure sectors are listed in this paragraph shall not be construed as an order of priority for consideration of the importance of such sectors.

"(3) TYPES OF THREAT.—The Board specifically shall consider the following types of threat to the critical infrastructure sectors described in paragraph (2), and to populations in all areas of the United States, urban and rural:

"(A) Biological threats.

"(B) Nuclear threats.

"(C) Radiological threats.

"(D) Incendiary threats.

"(E) Chemical threats.

"(F) Explosives.

"(G) Suicide bombers.

"(H) Cyber threats.

"(I) Any other threats based on proximity to specific past acts of terrorism or the known activity of any terrorist group.

The order in which the types of threat are listed in this paragraph shall not be construed as an order of priority for consideration of the importance of such threats.

"(4) CONSIDERATION OF ADDITIONAL FACTORS.—The Board shall take into account any other specific threat to a population (including a transient commuting or tourist population) or critical infrastructure sector that the Board has determined to exist. In evaluating the threat to a population or critical infrastructure sector, the Board shall give greater weight to threats of terrorism based upon their specificity and credibility, including any pattern of repetition.

"(5) RISK ANALYSIS AND ASSESSMENT.—Prior to evaluating and prioritizing all pending applications for covered grants, the Board shall provide an opportunity for applicants to provide information to the Board regarding the risk profile of the applicants' jurisdictions.

"(6) COORDINATION.—The Board shall coordinate with State, local, regional, and tribal officials in establishing criteria for evaluating and prioritizing applications for covered grants.

"(7) MINIMUM AMOUNTS.—After evaluating and prioritizing grant applications under paragraph (1), the Board shall ensure that, for each fiscal year—

"(A) each of the States, other than the Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands, that has an approved State homeland security plan receives no less than 0.25 percent of the funds available for covered grants for that fiscal year for purposes of implementing its homeland security plan in accordance with the prioritization of needs under section 2003(c)(1)(D);

"(B) each of the States, other than the Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands, that has an approved State homeland security plan and that meets one or both of the additional high-risk qualifying criteria under paragraph (8) receives no less than 0.45 percent of the funds available for covered grants for that fiscal year for purposes of implementing its homeland security plan in accordance with the prioritization of needs under section 2003(c)(1)(D);

"(C) the Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands each receives no less than 0.08 percent of the funds available for covered grants for that fiscal year for purposes of implementing its approved State homeland security plan in accordance with the prioritization of needs under section 2003(c)(1)(D); and

"(D) directly eligible tribes collectively receive no less than 0.08 percent of the funds available for covered grants for such fiscal year for purposes of addressing the needs identified in the applications of such tribes, consistent with the homeland security plan of each State within the boundaries of which any part of any such tribe is located, except that this clause shall not apply with respect to funds available for a fiscal year if the Secretary receives less than 5 applications for such fiscal year from such tribes under section 2003(e)(6)(A) or does not approve at least one such application.

"(8) ADDITIONAL HIGH-RISK QUALIFYING CRITERIA.—For purposes of paragraph (7)(B), additional high-risk qualifying criteria consist of—

"(A) having a significant international land border; or

"(B) adjoining a body of water within North America through which an international boundary line extends.

"(d) EFFECT OF REGIONAL AWARDS ON STATE MINIMUM.—Any regional award, or portion thereof, provided to a State under section 2003(e)(5)(C) shall not be considered in calculating the minimum State award under subsection (c)(7) of this section.

"SEC. 2005. USE OF FUNDS.

"(a) IN GENERAL.—A covered grant may be used for—

"(1) purchasing or upgrading equipment, including computer software, to enhance terrorism preparedness;

"(2) exercises to strengthen terrorism preparedness;

"(3) training for prevention (including detection) of, preparedness for, response to, or recovery from attacks involving weapons of mass destruction, including training in the use of equipment and computer software;

"(4) developing or updating State homeland security plans, risk assessments, mutual aid agreements, and emergency management plans to enhance terrorism preparedness;

"(5) establishing or enhancing mechanisms for sharing terrorism threat information;

"(6) systems architecture and engineering, program planning and management, strategy formulation and strategic planning, life-cycle systems design, product and technology evaluation, and prototype development for terrorism preparedness purposes;

"(7) additional personnel costs resulting from—

"(A) elevations in the threat alert level of the Homeland Security Advisory System by the Secretary, or a similar elevation in threat alert level issued by a State, region, or local government with the approval of the Secretary;

"(B) travel to and participation in exercises and training in the use of equipment and on prevention activities; and

"(C) the temporary replacement of personnel during any period of travel to and participation in exercises and training in the use of equipment and on prevention activities;

"(8) the costs of equipment (including software) required to receive, transmit, handle, and store classified information;

"(9) the costs of commercially available interoperable communications equipment (which, where applicable, is based on national, voluntary consensus standards) that the Secretary, in consultation with the Chairman of the Federal Communications Commission, deems best suited to facilitate interoperability, coordination, and integration between and among emergency communications systems, and that complies with prevailing grant guidance of the Department for interoperable communications;

"(10) educational curricula development for first responders to ensure that they are prepared for terrorist attacks;

"(11) training and exercises to assist public elementary and secondary schools in developing and implementing programs to instruct students regarding age-appropriate skills to prevent, prepare for, respond to, mitigate against, or recover from an act of terrorism;

"(12) paying of administrative expenses directly related to administration of the grant, except that such expenses may not exceed 3 percent of the amount of the grant;

"(13) paying for the conduct of any activity permitted under the Law Enforcement Terrorism Prevention Program, or any such successor to such program; and

"(14) other appropriate activities as determined by the Secretary.

"(b) PROHIBITED USES.—Funds provided as a covered grant may not be used—

"(1) to supplant State or local funds;

"(2) to construct buildings or other physical facilities, including barriers, fences, gates, and other such devices intended for the protection of critical infrastructure against potential attack, except those that are constructed under terms and conditions consistent with the requirements of section 611(j)(8) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5196(j)(8)), and the cost of which does not exceed the greater of—

"(A) $1,000,000 per project; or

"(B) such greater amount as may be approved by the Secretary, which may not exceed 10 percent of the total amount of the covered grant;

"(3) to acquire land; or

"(4) for any State or local government cost sharing contribution.

"(c) PERSONNEL COSTS.—A State and local government may use a covered grant to pay costs of personnel dedicated exclusively to counterterrorism and intelligence activities (including detection of, collection and analysis of intelligence relating to, investigation of, prevention of, and interdiction of suspected terrorist activities), if the hiring of such personnel is consistent with an applicable State homeland security plan.

"(d) MULTIPLE-PURPOSE FUNDS.—Nothing in this section shall be construed to preclude State and local governments from using covered grant funds in a manner that also enhances first responder preparedness for emergencies and disasters unrelated to acts of terrorism, if such use assists such governments in achieving essential capabilities for terrorism preparedness established by the Secretary.

"(e) REIMBURSEMENT OF COSTS.—(1) In addition to the activities described in subsection (a), a covered grant may be used to provide a reasonable stipend to paid-on-call or volunteer first responders who are not otherwise compensated for travel to or participation in training covered by this section. Any such reimbursement shall not be considered compensation for purposes of rendering such a first responder an employee under the Fair Labor Standards Act of 1938 (29 U.S.C. 201 et seq.).

"(2) An applicant for a covered grant may petition the Secretary for the reimbursement of the cost of any activity relating to prevention (including detection) of, preparedness for, response to, or recovery from acts of terrorism that is a Federal duty and usually performed by a Federal agency, and that is being performed by a State or local government (or both) under agreement with a Federal agency.

"(f) ASSISTANCE REQUIREMENT.—The Secretary may not require that equipment paid for, wholly or in part, with funds provided as a covered grant be made available for responding to emergencies in surrounding States, regions, and localities, unless the Secretary undertakes to pay the costs directly attributable to transporting and operating such equipment during such response.

"(g) COST SHARING.—

"(1) IN GENERAL.—The Federal share of the costs of an activity carried out with a covered grant to a State, region, or directly eligible tribe awarded after the 2-year period beginning on the date of the enactment of this section shall not exceed 75 percent.

"(2) INTERIM RULE.—The Federal share of the costs of an activity carried out with a covered grant awarded before the end of the 2-year period beginning on the date of the enactment of this section shall be 100 percent.

"(3) IN-KIND MATCHING.—Each recipient of a covered grant may meet the matching requirement under subparagraph (A) by making in-kind contributions of goods or services that are directly linked with the purpose for which the grant is made, as determined by the Secretary, including any necessary personnel overtime, contractor services, administrative costs, equipment fuel and maintenance, and rental space.".

(b) DEFINITION OF EMERGENCY RESPONSE PROVIDERS.—Paragraph (6) of section 2 of the Homeland Security Act of 2002 (Public Law 107–296; 6 U.S.C. 101(6)) is amended by striking "includes" and all that follows and inserting "includes Federal, State, and local governmental and nongovernmental emergency public safety, law enforcement, fire, emergency response, emergency medical (including hospital emergency facilities), and related personnel, organizations, agencies, and authorities.".

(c) SUPERSEDED PROVISION.—This section supersedes section 1014(c)(3) of Public Law 107–56.

SEC. 802. AUTHORIZATION OF APPROPRIATIONS.

Of the amount authorized to be appropriated under section 101 for fiscal year 2007, $2,900,000,000 is for making covered grants (as that term is defined in section 2001 of the Homeland Security Act of 2002, as added by section 801 for that fiscal year.

SEC. 803. METROPOLITAN MEDICAL RESPONSE SYSTEM.

(a) IN GENERAL.—There is in the Department of Homeland Security a Metropolitan Medical Response System. Under the System, the Assistant Secretary for Grants and Training shall administer grants to develop, maintain, and enhance medical preparedness systems that are capable of responding effectively during the initial hours of a public health crisis or mass-casualty event caused by an act of terrorism, natural disaster, or other emergency.

(b) USE OF FUNDS.—The Metropolitan Medical Response System shall make grants to local governments to enhance any of the following activities:

(1) Medical surge capacity.

(2) Mass prophylaxis.

(3) Chemical, biological, radiological, nuclear, and explosive detection, response, and decontamination capabilities.

(4) Emergency communications capabilities.

(5) Information sharing and collaboration capabilities.

(6) Regional collaboration.

(7) Triage and pre-hospital treatment.

(8) Medical supply management and distribution.

(9) Fatality management.

(10) Such other activities as the Secretary may provide.

(c) AUTHORIZATION OF APPROPRIATIONS.—Of the amount authorized under section 101, there is authorized to be appropriated to carry out this section $60,000,000.

TITLE IX—TRANSPORTATION SECURITY

Subtitle A—Rail and Public Transportation Security

SEC. 901. TRANSPORTATION SECURITY.

(a) IN GENERAL.—Title IV of the Homeland Security Act of 2002 (6 U.S.C. 201 et seq.) is amended by adding at the end the following new subtitle:

"Subtitle G—Transportation Security

"SEC. 481. RAIL AND PUBLIC TRANSPORTATION VULNERABILITY ASSESSMENTS AND SECURITY PLANS.

"(a) IN GENERAL.—

"(1) REQUIREMENT.—Not later than 1 year after the date of enactment of this subtitle, the Secretary, acting through the Transportation Security Administration, shall promulgate regulations that—

"(A) establish standards, protocols, and procedures for vulnerability assessments and security plans for rail and public transportation systems;

"(B) require a designated rail or public transportation system owner or operator (as designated under subsection (b)) to—

"(i) conduct an assessment of the vulnerability of the rail or public transportation system to an act of terrorism; and

"(ii) prepare and implement a security plan that addresses the vulnerabilities identified in the vulnerability assessment; and

"(C) set deadlines of no later than 2 years after the promulgation of the regulations for the completion of vulnerability assessments and security plans.

"(2) CONSULTATION.—In promulgating the regulations under paragraph (1) the Secretary shall consult with the Department of Transportation and other appropriate Federal agencies.

"(b) DESIGNATED RAIL OR PUBLIC TRANSPORTATION SYSTEM.—For the purposes of this subtitle, the term 'designated rail or public transportation system' means—

"(1) a heavy rail, light rail, commuter rail, or other freight or passenger rail system, including Federal and government sponsored entities;

"(2) a ferry system; or

"(3) an intracity or intercity bus system.

"(c) VULNERABILITY ASSESSMENTS.—

"(1) REQUIREMENTS.—For a rail or public transportation system designated under subsection (b), the Secretary shall provide assistance and guidance in conducting vulnerability assessments and shall require that the vulnerability assessments include at a minimum—

"(A) identification and evaluation of critical infrastructure and assets, including subway platforms, rail, bus, and ferry terminals, rail tunnels, rail bridges, rail switching and storage areas, and information systems; and

"(B) identification of vulnerabilities to the infrastructure and assets identified under subparagraph (A) in—

"(i) physical security;

"(ii) passenger and commuter security;

"(iii) programmable electronic devices, computers, computer or communications networks, or other automated systems which are used by the rail or public transportation system;

"(iv) alarms, cameras and other protection systems;

"(v) communications systems;

"(vi) utilities;

"(vii) contingency response; and

"(viii) other areas as determined by the Secretary.

"(2) THREAT INFORMATION.—

"(A) The vulnerability assessments under paragraph (1) shall incorporate any threat information as provided by the Secretary, and any other threat information relevant to the vulnerability of the rail or public transportation system.

"(B) The Secretary shall provide in a timely manner, to the maximum extent practicable under applicable authority and in the interests of national security, to the rail or public transportation system subject to the requirements in paragraph (1), threat information that is relevant to that rail or public transportation system, including an assessment of the most likely method that could be used by terrorists to exploit vulnerabilities, and their likelihood of success.

"(d) SECURITY PLANS.—

"(1) REQUIREMENTS.—For a rail or public transportation system designated under subsection (b), the Secretary shall provide assistance and guidance in preparing and implementing security plans and shall require that the security plan include at a minimum—

"(A) security measures to address the vulnerabilities identified in the vulnerability assessment required under subsection (c);

"(B) plans for periodic drills and exercises that include participation by local law enforcement agencies and first responders as appropriate;

"(C) equipment, plans, and procedures to be implemented or used by the rail or public transportation system in response to a terrorist attack, including evacuation and passenger communication plans;

"(D) identification of steps taken with State and local law enforcement agencies, first responders, and Federal officials to coordinate security measures and plans for response to a terrorist attack;

"(E) a description of training and exercises for employees of a rail or public transportation system, which includes, as appropriate, a strategy or timeline for training;

"(F) enhanced security measures to be taken when the Secretary declares a period of heightened security risk; and

"(G) other actions or procedures the Secretary determines are appropriate to address the vulnerability of a rail or public transportation system to a terrorist attack.

"(2) CONSISTENCY WITH OTHER PLANS.—Security plans shall be consistent with the requirements of the National Infrastructure Protection Plan (including any Transportation Sector Specific Plan) and the National Strategy for Transportation Security.

"(e) EXISTING PROCEDURES, PROTOCOLS, AND STANDARDS.—

"(1) DETERMINATION.—In response to a petition by a person, or at the discretion of the Secretary, the Secretary may endorse or recognize existing procedures, protocols, and standards that the Secretary determines to meet all or part of the requirements of this subtitle regarding vulnerability assessments and security plans.

"(2) REQUIREMENTS.—Upon review and written determination by the Secretary that existing procedures, protocols, or standards for a rail or public transportation system satisfy some or all of the requirements of this subtitle, any rail or public transportation system may elect to comply with those procedures, protocols, or standards.

"(3) PARTIAL APPROVAL.—If the Secretary finds that the existing procedures, protocols, and standards satisfy only part of the requirements of this subtitle, he may accept those submissions, but shall require submission of any additional information relevant to vulnerability assessments and security plans to ensure that the requirements of this subtitle are fulfilled.

"(4) NOTIFICATION.—If the Secretary does not endorse or recognize particular procedures, protocols, and standards, the Secretary shall provide to each person that submitted a petition under paragraph (1) a written notification that includes an explanation of the reasons why the endorsement or recognition was not made.

"(f) CO-LOCATED FACILITIES.—The Secretary shall permit the development and implementation of coordinated vulnerability assessments and security plans, at the discretion of a rail or public transportation system owner or operator, to the extent two or more rail or public transportation systems have shared facilities, such as tunnels, bridges, or stations, or facilities that are geographically close or otherwise co-located.

"(g) ENFORCEMENT.—Regulations promulgated under this section may be enforced by the Secretary through penalties authorized under section 114(u) of title 49, United States Code.

"SEC. 482. NATIONAL RAIL AND PUBLIC TRANSPORTATION SECURITY PLAN.

"(a) IN GENERAL.—The Secretary shall develop and implement, and update as appropriate, a supplement to the National Strategy for Transportation Security re-

quired under section 114(t) of title 49, United States Code to be entitled the 'National Rail and Public Transportation Security Plan'.

"(b) INCLUDED ELEMENTS.—The supplement required under subsection (a) shall—

"(1) include a description of the roles, responsibilities, and authorities of Federal, State, and local agencies, designated Federal and government sponsored entities, tribal governments, and appropriate rail and public transportation stakeholders, including nonprofit employee organizations that represent rail and public transportation system employees;

"(2) identify and address gaps and unnecessary overlaps in the roles, responsibilities, or authorities described in paragraph (1);

"(3) identify and make recommendations regarding legislative, regulatory, and organizational changes necessary to improve coordination among the entities described in paragraph (1) to enhance the security of rail and public transportation systems;

"(4) provide measurable goals, including objectives, mechanisms and a schedule, for enhancing the security of rail and public transportation systems;

"(5) include a process for sharing intelligence and information with the entities described in paragraph (1);

"(6) include a process for expediting security clearances to facilitate intelligence and information sharing with the entities described in paragraph (1);

"(7) describe current and future public outreach and educational initiatives designed to inform the public how to prevent, prepare for and respond to a terrorist attack on rail and public transportation systems;

"(8) include a framework for resuming the operation of rail and public transportation systems as soon as possible in the event of an act of terrorism;

"(9) include a strategy and timeline for the Department and other appropriate Federal agencies to research and develop new technologies, including advanced technologies with long term research and development timelines for securing rail and public transportation systems;

"(10) build on available resources and consider costs and benefits;

"(11) describe how the Department has reviewed the previous attacks on rail and public transportation systems throughout the world in the last 10 years, the lessons learned from this review, and how these lessons inform current and future efforts to secure rail and public transportation systems; and

"(12) expand upon, leverage, and relate to existing strategies and plans, including the National Infrastructure Protection Plan required by Homeland Security Presidential Directive-7.

"SEC. 483. RAIL AND PUBLIC TRANSPORTATION STRATEGIC INFORMATION SHARING PLAN.

"(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Transportation, shall develop and submit to the appropriate congressional committees no later than 90 days after the enactment of this subtitle a Rail and Public Transportation Strategic Information Sharing Plan to ensure the robust development of both tactical and strategic intelligence products pertaining to the threats and vulnerabilities to rail and public transportation systems for dissemination to Federal, State, and local agencies; tribal governments; and appropriate rail and public transportation stakeholders.

"(b) CONTENT OF PLAN.—The plan required under subsection (a) shall include—

"(1) a description of how intelligence analysts in the Transportation Security Administration are coordinating with other intelligence analysts in the Department and other Federal, State, and local agencies;

"(2) deadlines for the completion of any organizational changes within the Department to accommodate implementation of the plan; and

"(3) a description of resource needs for fulfilling the plan.

"(c) UPDATES.—

"(1) After the plan is provided under subsection (a), the Secretary shall certify to the appropriate congressional committees when the plan has been fully implemented.

"(2) After the Secretary provides the certification under paragraph (1), the Secretary shall provide a report to the appropriate congressional committees each year thereafter on the following:

"(A) The number and brief description of each rail and public transportation intelligence report created and disseminated under the plan.

"(B) The classification of each report as tactical or strategic.

"(C) The numbers of different government, law enforcement, and private sector partners who were provided with each intelligence product.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting at the end of the items relating to title IV the following:

"Subtitle G—Transportation Security

"Sec. 481. Rail and public transportation vulnerability assessments and security plans.
"Sec. 482. National rail and public transportation security plan.
"Sec. 483. Rail and public transportation strategic information sharing plan.".

SEC. 902. RULEMAKING REQUIREMENTS.

(a) INTERIM FINAL RULE AUTHORITY.—The Secretary of Homeland Security shall issue an interim final rule as a temporary regulation implementing section 481 of the Homeland Security Act of 2002, as added by section 901 of this title, as soon as practicable after the date of enactment of this Act, without regard to the provisions of chapter 5 of title 5, United States Code. All regulations prescribed under the authority of this subsection that are not earlier superseded by final regulations shall expire not later than 1 year after the date of enactment of this Act.

(b) INITIATION OF RULEMAKING.—The Secretary of Homeland Security may initiate a rulemaking to implement section 481 of the Homeland Security Act of 2002, as added by section 901 of this title, as soon as practicable after the date of enactment of this Act. The final rule issued pursuant to that rulemaking may supersede the interim final rule promulgated under this section.

SEC. 903. RAIL AND PUBLIC TRANSPORTATION SECURITY TRAINING PROGRAM.

(a) AMENDMENT.—Subtitle A of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 361) is amended by adding at the end the following new section:

"SEC. 802. RAIL AND PUBLIC TRANSPORTATION SECURITY TRAINING PROGRAM.

"(a) IN GENERAL.—The Secretary, acting through the appropriate Department official with primary responsibility for training programs, and in coordination with the Transportation Security Administration, shall develop and issue detailed guidance for a rail and public transportation worker security training program for the purpose of enhancing the capabilities of rail and public transportation workers, including front-line transit employees such as bus and rail operators, mechanics, customer service employees, maintenance employees, transit police, emergency response providers, and security personnel, to prevent, prepare for, respond to, mitigate against, and recover from threatened or actual acts of terrorism.

"(b) PROGRAM ELEMENTS.—The guidance developed under subsection (a) shall provide a program that—

"(1) includes, at a minimum, elements that address—

"(A) determination of the seriousness of any occurrence;

"(B) crew and passenger communication and coordination;

"(C) recognition of suspicious behavior or actions and appropriate response;

"(D) use of protective devices;

"(E) evacuation procedures (including passengers, workers, and those with disabilities);

"(F) training exercises regarding various threat conditions, including tunnel evacuation procedures; and

"(G) any other subject the Secretary considers appropriate;

"(2) is consistent with, and supports implementation of, the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goals, and other national initiatives;

"(3) considers existing training programs including Federal or industry programs; and

"(4) is evaluated against clear and consistent performance measures.

"(c) NATIONAL VOLUNTARY CONSENSUS STANDARDS.—The Secretary shall—

"(1) support the development, promulgation, and regular updating as necessary of national voluntary consensus standards for rail and public transportation security training; and

"(2) ensure that the training provided under this section is consistent with such standards.

"(d) TRAINING PARTNERS.—In developing and delivering training under the program under this section, the Secretary shall—

"(1) work with government training facilities, academic institutions, industry and private organizations, employee organizations, and other relevant entities that provide specialized, state-of-the-art training; and

"(2) utilize, as appropriate, training provided by industry, public safety academies, State and private colleges and universities, and other facilities.

"(e) UPDATES.—The Secretary shall regularly update the training guidance issued under subsection (a) to reflect new or different security threats.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (116 Stat. 2135) is amended by inserting after the item relating to section 801 the following:

"Sec. 802. Rail and public transportation security training program.".

SEC. 904. INTERAGENCY COOPERATION.

The Secretary of Homeland Security shall consider whether in fulfilling the requirements of this title, in order to promote communications, efficiency, and nonduplication of effort, memoranda of agreement should be updated or executed with other Federal agencies, including the Department of Transportation, or between entities of the Department and other Federal entities, including between the Transportation Security Administration and the Federal Transit Administration, the Pipeline and Hazardous Materials Safety Administration, and the Federal Railroad Administration.

SEC. 905. RAIL AND PUBLIC TRANSPORTATION SECURITY GRANT PROGRAM.

(a) AMENDMENT.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.) is amended by adding at the end the following new section:

"SEC. 514. RAIL AND PUBLIC TRANSPORTATION SECURITY GRANT PROGRAM.

"(a) GRANTS AUTHORIZED.—The Secretary, acting through the Department official with primary responsibility for grants and training, shall establish a grant program to allocate Federal homeland security assistance administered by the Department to United States rail and public transportation systems designated under section 481 on the basis of risk and need.

"(b) PRIORITIZATION PROCESS.—In awarding grants under this section, the Secretary shall conduct an assessment of United States rail and public transportation systems to develop a prioritization for awarding grants authorized under subsection (a) based upon—

"(1) the most current risk assessment available from the Department, incorporating threat, vulnerability, and consequence analysis;

"(2) the national economic and strategic defense considerations of individual rail and public transportation systems; and

"(3) any other factors that the Secretary determines to be appropriate.

"(c) APPLICATION.—

"(1) IN GENERAL.—Any rail or public transportation security system subject to the requirements of section 481 may submit an application for a grant under this section, at such time, in such form, and containing such information and assurances as the Secretary may require.

"(2) MINIMUM STANDARDS FOR PAYMENT OR REIMBURSEMENT.—Each application submitted under paragraph (1) shall include—

"(A) a comprehensive description of—

"(i) the purpose of the project for which the applicant seeks a grant under this section and why the applicant needs the grant;

"(ii) the applicability of the project to the security plan prepared under section 481 and other homeland security plans;

"(iii) any existing cooperation or mutual aid agreements with other rail or public transportation systems, organizations, or State, and local governments as such agreements relate to rail and public transportation security; and

"(iv) a capital budget showing how the applicant intends to allocate and expend the grant funds; and

"(B) a determination by the Transportation Security Administration that the project—

"(i) addresses or corrects rail and public transportation security vulnerabilities; and

"(ii) helps to ensure compliance with the security plan prepared under section 481.

"(3) PROCEDURAL SAFEGUARDS.—The Secretary, in consultation with the Office of the Inspector General and the Department official with primary responsibility for grants and training, shall issue guidelines to establish appropriate accounting, reporting, and review procedures to ensure that—

"(A) grant funds are used for the purposes for which they were made available;

"(B) grantees have properly accounted for all expenditures of grant funds; and

"(C) grant funds not used for such purposes and amounts not obligated or expended are returned.

"(d) USE OF FUNDS.—Grants awarded under this section may be used—

"(1) to help implement security plans prepared under section 481;

"(2) to remedy rail and public transportation security vulnerabilities identified through vulnerability assessments approved by the Secretary;

"(3) for non-Federal projects contributing to the overall security of a rail or public transportation security system, as determined by the Secretary;

"(4) for the salaries, benefits, overtime compensation, and other costs of additional security personnel for State and local agencies for activities required by the security plan prepared under section 481;

"(5) for the cost of acquisition, operation, and maintenance of equipment that contributes to the overall security of the rail and public transportation security system, if the need is based upon vulnerability assessments approved by the Secretary or identified in a security plan prepared under section 481;

"(6) to conduct vulnerability assessments approved by the Secretary;

"(7) to purchase or upgrade equipment, including communications equipment that is interoperable with Federal, State, and local agencies and tribal governments; and computer software, to enhance terrorism preparedness;

"(8) to conduct exercises or training for prevention and detection of, preparedness for, response to, or recovery from acts of terrorism;

"(9) to establish or enhance mechanisms for sharing terrorism threat information and to ensure that the mechanisms are interoperable with Federal, State, and local agencies and tribal governments;

"(10) for the cost of equipment (including software) required to receive, transmit, handle, and store classified information; and

"(11) for the protection of critical infrastructure against potential attack by the addition of barriers, fences, gates, and other such devices, except that the cost of such measures may not exceed the greater of—

"(A) $1,000,000 per project; or

"(B) such greater amount as may be approved by the Secretary, which may not exceed 10 percent of the total amount of the grant.

"(e) REIMBURSEMENT OF COSTS.—An applicant for a grant under this section may petition the Secretary for the reimbursement of the cost of any activity relating to prevention (including detection) of, preparedness for, response to, or recovery from acts of terrorism that is a Federal duty and usually performed by a Federal agency, and that is being performed by a State or local government (or both) under agreement with a Federal agency.

"(f) PROHIBITED USES.—Grants awarded under this section may not be used to—

"(1) supplant State or local funds for activities of the type described in subsection (d);

"(2) to construct buildings or other physical facilities, including barriers, fences, gates, and other such devices intended for the protection of critical infrastructure against potential attack, except those that are constructed under terms and conditions consistent with the requirements of section 611(j)(8) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5196(j)(8)), and the cost of which does not exceed the greater of—

"(A) $1,000,000 per project; or

"(B) such greater amount as may be approved by the Secretary, which may not exceed 10 percent of the total amount of the covered grant;

"(3) acquire land; or

"(4) make any State or local government cost-sharing contribution.

"(g) MATCHING REQUIREMENT.—

"(1) IN GENERAL.—Except as provided in subparagraph (A) or (B) of paragraph (2), Federal funds for any eligible project under this section shall not exceed 75 percent of the total cost of such project.

"(2) EXCEPTIONS.—

"(A) SMALL PROJECTS.—The requirement of paragraph (1) shall not apply with respect to a project with a total cost of not more than $25,000.

"(B) HIGHER LEVEL OF FEDERAL SUPPORT REQUIRED.—The requirement of paragraph (1) shall not apply with respect to a project if the Secretary determines that the project merits support and cannot be undertaken without a higher rate of Federal support than the rate described in paragraph (1).

"(3) IN-KIND CONTRIBUTIONS.—Each recipient of a grant under this section may meet the requirement of paragraph (1) by making in-kind contributions of goods or services that are directly linked with the purpose for which the grant is made, as determined by the Secretary, including any necessary personnel expenses, contractor services, administrative costs, equipment, fuel, or maintenance, and rental space.

"(h) MULTIPLE PHASE PROJECTS.—

"(1) IN GENERAL.—The Secretary may award grants under this section for projects that span multiple years.

"(2) FUNDING LIMITATION.—Not more than 20 percent of the total grant funds awarded under this section in any fiscal year may be awarded for projects that span multiple years.

"(i) CONSISTENCY WITH PLANS.—The Secretary shall ensure that each grant awarded under this section—

"(1) is used to supplement and support, in a consistent and coordinated manner, the applicable security plan; and

"(2) is consistent and coordinated with any applicable State or Urban Area Homeland Security Plan.

"(j) COORDINATION AND COOPERATION.—The Secretary shall ensure that all projects that receive grant funding under this section within any area defined in an Urban Area Homeland Security Plan are coordinated with other projects in such area.

"(k) REVIEW AND AUDITS.—The Secretary shall require all grantees under this section to maintain such records as the Secretary may require and make such records available for review and audit by the Secretary, the Comptroller General of the United States, or the Inspector General of the Department.

"(l) QUARTERLY REPORTS REQUIRED AS A CONDITION OF HOMELAND SECURITY GRANTS.—

"(1) EXPENDITURE REPORTS REQUIRED.—As a condition of receiving a grant under this section, the Secretary shall require the grant recipient to submit quarterly reports to the Secretary that describe each expenditure made by the recipient using grant funds.

"(2) DEADLINE FOR REPORTS.—Each report required under paragraph (1) shall be submitted not later than 30 days after the last day of a fiscal quarter and shall describe expenditures made during that fiscal quarter.

"(3) PUBLICATION OF EXPENDITURES.—

"(A) IN GENERAL.—Not later than 1 week after receiving a report under this subsection, the Secretary shall publish and make publicly available on the Internet website of the Department a description of each expenditure described in the report.

"(B) WAIVER.—The Secretary may waive the requirement of subparagraph (A) if the Secretary determines that it is in the national security interests of the United States to do so.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (116 Stat. 2135) is amended by adding after item relating to section 513 (as added by section 602(b)) the following:

"Sec. 514. Rail and public transportation security grant program.".

SEC. 906. RAIL AND PUBLIC TRANSPORTATION SECURITY EXERCISE PROGRAM.

(a) Subtitle A of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 361) is amended by adding at the end the following new section:

"SEC. 803. RAIL AND PUBLIC TRANSPORTATION SECURITY EXERCISE PROGRAM.

"(a) IN GENERAL.—The Secretary, acting through the Department official with primary responsibility for grants and training, shall establish a Rail and Public Transportation Security Exercise Program (hereinafter in this section referred to as the 'Program') for the purpose of testing and evaluating the capabilities of Federal, State, and local agencies and tribal governments, rail and public transportation system employees and management, governmental and nongovernmental emergency response providers, the private sector, or any other organization or entity, as the Secretary determines to be appropriate, to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism, natural disasters, and other emergencies at rail and public transportation systems.

"(b) REQUIREMENTS.—The Secretary, acting through the Department official with primary responsibility for grants and training, and in coordination with the Assistant Secretary of Homeland Security (Transportation Security Administration), shall ensure that the Program—

"(1) consolidates all existing rail and public transportation system security exercise programs administered by the Department;

"(2) conducts, on a periodic basis, exercises at rail and public transportation systems that are—

"(A) scaled and tailored to the needs of each rail and public transportation system;

"(B) live in the case of the most at-risk rail and public transportation systems;

"(C) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;

"(D) consistent with the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the Na-

tional Preparedness Guidance, the National Preparedness Goal, and other such national initiatives;

"(E) evaluated against clear and consistent performance measures;

"(F) assessed to learn best practices, which shall be shared with appropriate Federal, State, local and tribal officials, rail and public transportation system employees and management; governmental and nongovernmental emergency response providers, and the private sector; and

"(G) followed by remedial action in response to lessons learned; and

"(3) assists State and local governments and rail and public transportation systems in designing, implementing, and evaluating exercises that—

"(A) conform to the requirements of paragraph (2); and

"(B) are consistent with any applicable State or Urban Area Homeland Security Plan.

"(c) REMEDIAL ACTION MANAGEMENT SYSTEM.—The Secretary, acting through the Department official with primary responsibility for grants and training, shall establish a Remedial Action Management System to—

"(1) identify and analyze each rail and public transportation system exercise for lessons learned and best practices;

"(2) disseminate lessons learned and best practices to participants in the Program;

"(3) monitor the implementation of lessons learned and best practices by participants in the Program; and

"(4) conduct remedial action tracking and long-term trend analysis.

"(d) GRANT PROGRAM FACTOR.—In evaluating and prioritizing applications for Federal financial assistance under section 513, the Secretary shall give additional consideration to those applicants that have conducted rail and public transportation security exercises under this section.

"(e) CONSULTATION.—The Secretary shall ensure that, in carrying out the Program, the Department official with primary responsibility for grants and training shall consult with—

"(1) a geographic and substantive cross section of governmental and nongovernmental emergency response providers; and

"(2) rail and public transportation system personnel and management.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (116 Stat. 2135) is amended by inserting after the item relating to section 802 (as added by section 903(b)) the following:

"Sec. 803. Rail and public transportation security exercise program.".

SEC. 907. AUTHORIZATION OF APPROPRIATIONS.

Of the amount authorized to be appropriated under section 101 for fiscal year 2007, $400,000,000 is for grants and assistance to improve rail and public transportation security for that fiscal year.

Subtitle B—Transportation Security Operations Enhancements

SEC. 911. AVIATION SECURITY FUNDING.

Section 48301 of title 49, United States Code, is amended to read as follows:

"§ 48301. Aviation security funding

"There are authorized to be appropriated for fiscal years 2006, 2007, 2008, 2009, and 2010 such sums as may be necessary to carry out chapter 449 and related aviation security activities under this title.".

SEC. 912. RESEARCH AND DEVELOPMENT OF TRANSPORTATION SECURITY TECHNOLOGY.

Section 137 of the Aviation and Transportation Security Act (49 U.S.C. 44912 note; 115 Stat. 637) is amended—

(1) in the first sentence of subsection (a) by striking "2002 through 2006" and inserting "2006 through 2010";

(2) in the first sentence of subsection (a) by striking "aviation" and inserting "transportation";

(3) by striking in the second sentence of subsection (a) "2002 and 2003" and inserting "2006 through 2010";

(4) by striking in subsection (a)(4) "aircraft" and inserting "transportation vehicles";

(5) in subsection (a)(5)—

(A) by striking "airport" and inserting "transportation"; and

(B) by inserting after "airports" the following: "and other transportation terminals and ports";

(6) in subsection (a)(6) by striking "airport" and inserting "transportation";

(7) in subsection (a)(7)—

(A) by striking "evaluation of aircraft" and inserting "evaluation of conveyance"; and

(B) by striking "vulnerability of aircraft" and inserting "vulnerability of conveyances"; and

(8) in the second sentence of subsection (b) by striking "Transportation Security Administration" and inserting "Department of Homeland Security".

SEC. 913. ENFORCEMENT AUTHORITY IN NONAVIATION TRANSPORTATION.

(a) Section 114 of title 49, United States Code, is amended by adding at the end the following:

"(u) CIVIL PENALTIES AND ENFORCEMENT OF REGULATIONS AND ORDERS OF THE SECRETARY OF HOMELAND SECURITY UNDER THIS TITLE OTHER THAN CHAPTER 449.—

"(1) APPLICATION.—This subsection applies to the enforcement of regulations prescribed, and orders issued, by the Secretary of Homeland Security under this title (other than chapter 449). Penalties for violation of regulations prescribed, and orders issued, by the Secretary of Homeland Security under chapter 449 of this title are provided under chapter 463 of this title.

"(2) GENERAL PENALTY.—(A) A person is liable to the United States Government for a civil penalty of not more than $10,000 for a violation of a regulation prescribed, or order issued, by the Secretary of Homeland Security under an applicable provision of this title.

"(B) A separate violation occurs under this paragraph for each day the violation continues.

"(3) ADMINISTRATIVE IMPOSITION OF CIVIL PENALTIES.—(A) The Secretary of Homeland Security may impose a civil penalty for a violation of a regulation prescribed, or order issued, under an applicable provision of this title. The Secretary shall give written notice of the finding of a violation and the penalty.

"(B) In a civil action to collect a civil penalty imposed by the Secretary under this paragraph, the issues of liability and the amount of the penalty may not be reexamined.

"(C) Notwithstanding subparagraph (a) of this paragraph, the district courts of the United States have exclusive jurisdiction of a civil action involving a penalty that the secretary initiates if—

"(i) the amount in controversy is more than—

"(I) $ 400,000 if the violation was committed by a person other than an individual or small business concern; or

"(II) $ 50,000 if the violation was committed by an individual or small business concern;

"(ii) the action is in rem or another action in rem based on the same violation has been brought; or

"(iii) another action has been brought for an injunction based on the same violation.

"(D) The maximum penalty the Secretary may impose under this paragraph is—

"(i) $400,000 if the violation was committed by a person other than an individual or small business concern; or

"(ii) $50,000 if the violation was committed by an individual or small business concern.

"(4) COMPROMISE AND SETOFF.—(A) The Secretary may compromise the amount of a civil penalty imposed under this subsection.

"(B) The Government may deduct the amount of a civil penalty imposed or compromised under this subsection from amounts it owes the person liable for the penalty.

"(5) INVESTIGATIONS AND PROCEEDINGS.—The provisions set forth in chapter 461 of this title shall be applicable to investigations and proceedings brought under this subsection to the same extent that they are applicable to investigations and proceedings brought with respect to aviation security duties designated to be carried out by the Secretary.

"(6) NONAPPLICATION.—Paragraphs (1) through (4) of this subsection do not apply to the following persons, who shall be subject to penalties as determined by the Secretary of Defense or the designee of the Secretary of Defense:

"(A) The transportation of personnel or shipments of materials by contractors where the Department of Defense has assumed control and responsibility.

"(B) A member of the armed forces of the United States when performing official duties.

"(C) A civilian employee of the Department of Defense when performing official duties.

"(7) LIMITATION.—For purposes of this subsection, the term 'person' does not include an employee of the United States Postal Service when performing official duties.

"(8) SMALL BUSINESS CONCERN DEFINED.—For purposes of this subsection, the term 'small business concern' has the meaning given that term in section 3 of the Small Business Act (15 U.S.C. 632).".

(b) Section 46301(a)(4) of title 49, United States Code is amended by striking "or another requirement under this title administered by the Under Secretary of Transportation for Security".

SEC. 914. LIABILITY FOR SECURITY SCREENING INSPECTIONS.

Section 44901 of title 49, United States Code, is amended by adding at the end the following:

"(i) LIABILITY FOR SECURITY SCREENING INSPECTIONS.—

"(1) LIMITATION FOR GOOD FAITH INSPECTIONS.—No officer or employee of the United States inspecting any person or property pursuant to section 44901 or 44903 shall be held liable for any civil damages as a result of such inspection if the officer or employee performed the inspection in good faith.

"(2) LIMITATION ON STATUTORY CONSTRUCTION.—Nothing in this subsection shall be construed to impair any defense otherwise available to an officer or employee described in paragraph (1) under statute or common law, including any defense of absolute or qualified immunity.

"(3) EXCLUSIVE REMEDY.—The exclusive remedy against the United States or its officers or employees for any damages arising from the loss, damage, detention, or negligent handling of property subject to security screening operations under section 44901 or 44903 shall be a claim pursuant to section 3723 of title 31, except that the maximum amount for which such a claim may be settled under section 3723(a) of title 31 shall be the same as the level established under section 254.4 of title 14, Code of Federal Regulations.".

SEC. 915. TEMPORARY PRIVATE SCREENER ASSISTANCE.

Section 44920 of title 49, United States Code, is amended adding at the end the following:

"(h) EMERGENCY SUPPLEMENTAL SCREENING.—The Secretary of Homeland Security may establish a program under which the screening of passengers and property at an airport under section 44901 may be supplemented for periods of limited duration in case of emergencies, such as natural disasters, terrorist acts, or threats to national security, by the screening personnel of a qualified private screening company in accordance with subsections (c) and (d) under a contract entered into with the Secretary.".

SEC. 916. RECURRENT TRAINING TO OPERATE CERTAIN AIRCRAFT.

Section 44939 of title 49, United States Code, is amended—

(1) in subsection (f), by inserting "and (g)" after "subsections (a) through (d)"; and

(2) in subsection (g)—

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

(B) by inserting after paragraph (1) the following:

"(2) RECURRENT TRAINING.—The Secretary may assess a fee for a threat assessment to determine that an alien as defined in this section, or any other individual specified by the Secretary, applying for recurrent training in the operation of any aircraft having a maximum certificated takeoff weight of more than 12,500 pounds is properly identified and has not since the time of any prior threat assessment conducted pursuant to this section become a present risk to aviation or national security. If the Secretary determines that such individual is a present risk to aviation or national security the Secretary shall immediately notify the person providing the training of the determination and that person shall not provide the training or if such training has commenced that person shall immediately terminate the training. Such fee shall not exceed the amount assessed under paragraph (1) and shall be promulgated by notice in the Federal Register.".

SEC. 917. ANNUAL REPORT ON UNCLAIMED MONEY RECOVERED.

The Secretary of Homeland Security shall ensure that the Department of Homeland Security maintains an accounting of monies retained under section 44945 of title 49, United States Code.

Subtitle C—Passenger Screening

SEC. 921. PASSENGER IDENTIFICATION DOCUMENTS.

(a) IN GENERAL.—Title IV of the Homeland Security Act of 2002 (6 U.S.C. 201 et seq.) is amended by inserting after section 483 (as added by section 901(a) of this Act) the following:

"SEC. 484. PASSENGER IDENTIFICATION DOCUMENTS.

"(a) IN GENERAL.—Not later than 180 days after the date of enactment of this section, the Assistant Secretary of Homeland Security (Transportation Security Administration) shall issue regulations to require a passenger to present an acceptable personal identification document for inspection before entering a sterile area of an airport in the United States. Such inspections shall be carried out by personnel designated by the Assistant Secretary.

"(b) ACCEPTABLE PERSONAL IDENTIFICATION DOCUMENTS.—

"(1) IN GENERAL.—In carrying out subsection (a), the Assistant Secretary shall establish a list of acceptable personal identification documents.

"(2) MINIMUM REQUIREMENTS.—The Assistant Secretary may include a personal identification document on the list to be established under paragraph (1) only if the document is issued under the authority of the United States Government, a State, or a foreign government and includes each of the following:

"(A) The individual's full legal name.

"(B) The individual's date of birth.

"(C) The individual's gender.

"(D) A photograph of the individual.

"(E) The individual's signature.

"(F) Physical security features designed to prevent tampering, counterfeiting, and duplication of the document for fraudulent purposes.

"(3) DRIVERS' LICENSES AND PERSONAL IDENTIFICATION CARDS.—The Assistant Secretary shall include on the list to be established under paragraph (1) drivers' licenses and personal identification cards that meet the requirements of section 202 of the Real ID Act of 2005 (49 U.S.C. 30301 note).

"(c) PROCEDURES AND STANDARDS.—In carrying out subsection (a), the Assistant Secretary shall establish—

"(1) procedures to match the name on a personal identification document with the name on an airline boarding document;

"(2) procedures to match the photograph on a personal identification document with the passenger presenting the document; and

"(3) standards for training personnel who check personal identification documents to recognize unacceptable and false identification documents.

"(d) FAILURE TO PRESENT ACCEPTABLE IDENTIFICATION DOCUMENTS.—A passenger attempting to enter a sterile area of an airport in the United States who does not present an acceptable identification document shall be subject to such additional security screening as the Assistant Secretary determines to be appropriate before the passenger may be admitted to the sterile area.

"(e) KNOWING PRESENTATION OF FALSE IDENTIFICATION DOCUMENTS; PENALTIES.—A passenger who knowingly presents a false identification document in an attempt to enter a sterile area of an airport in the United States shall be fined under title 18, United States Code, imprisoned for not more than 5 years, or both.

"(f) DEFINITIONS.—In this section, the following definitions apply:

"(1) FALSE.—The term 'false' has the meaning given such term by section 1028(d) of title 18, United States Code.

"(2) PASSENGER.—The term 'passenger' means an individual to be carried aboard a passenger aircraft to be operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation (as such terms are defined in section 40102 of title 49, United States Code).

"(3) STERILE AREA.—The term 'sterile area' means any part of an airport that is regularly accessible to passengers after having cleared a passenger security checkpoint.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding at the end of the items relating to subtitle G of title IV (as added by section 901(b)) the following:

"Sec. 484. Passenger identification documents.".

SEC. 922. INTERNATIONAL PASSENGER PRESCREENING.

Before issuing final regulations to amend the rules regarding the manner in which international passenger manifest data is transmitted by air carriers to Customs and Border Protection pursuant to section 44909(c) of title 49, United States

Code, the Secretary of Homeland Security shall conduct a pilot program to evaluate the use of automated systems for the immediate prescreening of passengers on flights in foreign air transportation, and shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report containing the following:

(1) An assessment of the technical performance of the tested system, including the system's accuracy, scalability, and effectiveness with respect to measurable factors, including, at a minimum, passenger throughput, the rate of flight diversions, and the rate of false negatives and positives.

(2) A description of the provisions of the tested systems to protect the civil liberties and privacy rights of passengers, as well as a description of the adequacy of an immediate redress or appeals process for passengers denied authorization to travel.

(3) Cost projections for implementation of the tested systems, including—

(A) projected costs to the Department of Homeland Security; and

(B) projected costs of compliance to air carriers operating flights described in subsection (a).

SEC. 923. INTERNATIONAL COOPERATIVE EFFORTS.

To ensure that the collection of passenger information is standardized among nations, the Secretary of Homeland Security is encouraged to pursue international cooperative efforts in the appropriate forum to set technology standards for passenger data and collection systems.

SEC. 924. COMPUTER ASSISTED PASSENGER PRESCREENING SYSTEM.

(a) REPORT.—Not later than 6 months after the date of the enactment of this Act, the Assistant Secretary of Homeland Security (Transportation Security Administration) shall submit to the Committee on Homeland Security of the House of Representatives and the Committees on Homeland Security and Governmental Affairs and Commerce, Science, and Transportation of the Senate a report containing—

(1) information on the percentage of airline passengers that are designated for secondary search on a daily basis by the Computer Assisted Passenger Prescreening System (in this section referred to as "CAPPS");

(2) information on the percentage of such airline passengers that have been found to be terrorists or associates of terrorists;

(3) information on the annual cost of administering CAPPS; and

(4) an evaluation of whether CAPPS screening should be continued after the full deployment of the Secure Flight program.

(b) FORM OF REPORT.—The report prepared under this section may be submitted in a classified form.

(c) LIMITATION ON SECONDARY SCREENING.—The Assistant Secretary, in cooperation with appropriate Federal agencies and the representatives of the aviation industry, shall develop a process to ensure that a passenger who has successfully completed a finger-print based background check conducted by the Department of Homeland Security, or holds a security clearance issued by the Department of Homeland Security, is not subject to secondary screening as the result of a designation under CAPPS.

SEC. 925. FEDERAL FLIGHT DECK OFFICERS.

(a) TRAINING AND REQUALIFICATION TRAINING.—Section 44921(c) of title 49, United States Code, is amended by adding at the end the following:

"(3) DATES OF TRAINING.—The Assistant Secretary shall ensure that a pilot who is eligible to receive Federal flight deck officer training is offered, to the maximum extent practicable, a choice of training dates and is provided at least 30 days advance notice of the dates.

"(4) TRAVEL TO TRAINING FACILITIES.—The Assistant Secretary shall establish a program to improve travel access to Federal flight deck officer training facilities through the use of charter flights or improved scheduled air carrier service.

"(5) REQUALIFICATION AND RECURRENT TRAINING.—

"(A) STANDARDS.—The Assistant Secretary shall establish qualification standards for facilities where Federal flight deck officers can receive requalification and recurrent training.

"(B) LOCATIONS.—The Assistant Secretary shall provide for requalification and recurrent training at geographically diverse facilities, including Federal, State, and local law enforcement and government facilities, and private training facilities that meet the qualification standards established under subparagraph (A).

"(6) COSTS OF TRAINING.—

"(A) IN GENERAL.—The Assistant Secretary shall provide Federal flight deck officer training, requalification training, and recurrent training to eligible pilots at no cost to the pilots or the air carriers that employ the pilots.

"(B) TRANSPORTATION AND EXPENSES.—The Assistant Secretary may provide travel expenses to a pilot receiving Federal flight deck officer training, requalification training, or recurrent training.

"(7) COMMUNICATIONS.—Not later than 180 days after the date of enactment of this paragraph, the Assistant Secretary shall establish a secure means for personnel of the Transportation Security Administration to communicate with Federal flight deck officers, and for Federal flight deck officers to communicate with each other, in support of the mission of such officers. Such means of communication may include a secure Internet website.".

(b) REVOCATION OF DEPUTIZATION OF PILOT AS FEDERAL FLIGHT DECK OFFICER.—Section 44921(d)(4) of such title is amended to read as follows:

"(4) REVOCATION.—

"(A) ORDERS.—The Assistant Secretary may issue, for good cause, an order revoking the deputization of a Federal flight deck officer under this section. The order shall include the specific reasons for the revocation.

"(B) HEARINGS.—An individual who is adversely affected by an order of the Assistant Secretary under subparagraph (A) is entitled to a hearing on the record. When conducting a hearing under this subparagraph, the administrative law judge shall not be bound by findings of fact or interpretations of laws and regulations of the Assistant Secretary.

"(C) APPEALS.—An appeal from a decision of an administrative law judge as a result of a hearing under subparagraph (B) shall be made to the Secretary of Homeland Security or the Secretary's designee.

"(D) JUDICIAL REVIEW OF A FINAL ORDER.—The determination and order of the Secretary revoking the deputization of a Federal flight deck officer under this section shall be final and conclusive unless the individual against whom such an order is issued files an application for judicial review under subchapter II of chapter 5 of title 5 (popularly known as the Administrative Procedure Act) within 60 days of entry of such order in the appropriate United States court of appeals.".

(c) FEDERAL FLIGHT DECK OFFICER FIREARM CARRIAGE PILOT PROGRAM.—Section 44921(f) of such title is amended by adding at the end the following:

"(4) PILOT PROGRAM.—

"(A) IN GENERAL.—Not later than 90 days after the date of enactment of this paragraph, the Assistant Secretary shall implement a pilot program to allow pilots participating in the Federal flight deck officer program to transport their firearms on their persons. The Assistant Secretary may prescribe any training, equipment, or procedures that the Assistant Secretary determines necessary to ensure safety and maximize weapon retention.

"(B) REVIEW.—Not later than 1 year after the date of initiation of the pilot program, the Assistant Secretary shall conduct a review of the safety record of the pilot program and transmit a report on the results of the review to Congress.

"(C) OPTION.—If the Assistant Secretary as part of the review under subparagraph (B) determines that the safety level obtained under the pilot program is comparable to the safety level determined under existing methods of pilots carrying firearms on aircraft, the Assistant Secretary shall allow all pilots participating in the Federal flight deck officer program the option of carrying their firearm on their person subject to such requirements as the Assistant Secretary determines appropriate.".

(d) FEDERAL FLIGHT DECK OFFICERS ON INTERNATIONAL FLIGHTS.—

(1) AGREEMENTS WITH FOREIGN GOVERNMENTS.—The President is encouraged to pursue aggressively agreements with foreign governments to allow maximum deployment of Federal flight deck officers on international flights.

(2) REPORT.—Not later than 180 days after the date of enactment of this Act, the President (or the President's designee) shall submit to Congress a report on the status of the President's efforts to allow maximum deployment of Federal flight deck officers on international flights.

(e) REFERENCES TO UNDER SECRETARY.—Section 44921 of title 49, United States Code, is amended—

(1) in subsection (a) by striking "Under Secretary of Transportation for Security" and inserting "Assistant Secretary of Homeland Security (Transportation Security Administration)";

(2) by striking "Under Secretary" each place it appears and inserting "Assistant Secretary"; and

(3) by striking "Under Secretary's" each place it appears and inserting "Assistant Secretary's".

SEC. 926. ENHANCED PERIMETER SECURITY AND ACCESS CONTROL THROUGH COMPREHENSIVE SCREENING OF AIRPORT WORKERS.

(a) PILOT PROGRAM.—Not later than 120 days after the date of enactment of this Act, the Assistant Secretary of Homeland Security (Transportation Security Administration) shall implement a pilot program at 5 commercial service airports to physically screen all airport workers with access to secure and sterile areas of the airport.

(b) PARTICIPATING AIRPORTS.—At least 2 of the airports participating in the pilot program shall be large hub airports (as defined in section 40102 of title 49, United States Code). Each of the remaining airports participating in the pilot program shall represent a different airport security risk category (as defined by the Assistant Secretary).

(c) SCREENING STANDARDS.—Screening for airport workers under the pilot program shall be conducted under the same standards as apply to individuals at airport security screening checkpoints, and shall be carried out by contract screeners at a minimum of 2 airports.

(d) DURATION.—The pilot program shall be carried out for a period of not less than 180 days.

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary to carry out this section.

(f) REPORT.—

(1) IN GENERAL.—Not later than 90 days after the last day of the pilot program, the Assistant Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on the results of the pilot program.

(2) CONTENTS.—The report shall contain, at a minimum, the following:

(A) An assessment of the impact of physically screening all airport workers with access to secure and sterile airport areas on screening and logistical resources.

(B) An assessment of the security improvements that are achieved from comprehensively screening such workers.

(C) An assessment of the costs of comprehensively screening such workers.

SEC. 927. PROHIBITED ITEMS.

The Assistant Secretary of Homeland Security (Transportation Security Administration) shall prohibit scissors of any length (except ostomy scissors shorter than four inches) and tools (including screwdrivers, wrenches and pliers) from being carried aboard a passenger aircraft operated by an air carrier or foreign air carrier in air transportation or interstate air transportation.

SEC. 928. SECURED AREAS OF AIRPORTS.

(a) IMPLEMENTATION OF IMPROVED AIRPORT PERIMETER ACCESS SECURITY.—Not later than one year after the date of the enactment of this Act, the Assistant Secretary of Homeland Security (Transportation Security Administration) shall issue regulations, directives, or other appropriate measures to implement the requirements of section 44903(h)(4) of title 49, United States Code.

(b) AIRPORT SECURITY PLANS.—The Assistant Secretary shall set a schedule for requiring airports to update their airport security plans to comply with the requirements of section 44903(h)(4) not later than three years after the issuance of the regulations, directives, or other measures required under subsection (a).

SEC. 929. REPAIR STATIONS.

(a) IMPLEMENTATION OF REGULATIONS FOR FOREIGN REPAIR STATIONS.—Not later than 90 days after the date of the enactment of this Act, the Assistant Secretary of Homeland Security (Transportation Security Administration) shall issue regulations, directives or other appropriate measures to implement the requirements of section 44924 of title 49, United States Code.

(b) REPORTS.—If the Assistant Secretary fails to comply with subsection (a), the Assistant Secretary shall notify in writing the appropriate congressional committees and shall publish in the Federal Register the Department's reasons for missing the deadline and an update of the progress towards meeting the requirements of subsection (a), once a week for every week that the noncompliance continues.

Subtitle D—Technical Amendments

SEC. 931. REPORTING REQUIREMENTS REPEALED.

The following provisions are repealed:

(1) Sections 607 and 608 of the Vision 100—Century of Aviation Reauthorization Act (49 U.S.C. 44903 note; 117 Stat. 2568).

(2) Section 109(b) of the Aviation and Transportation Security Act (49 U.S.C. 114 note; 115 Stat. 614).

(3) Section 44942 of title 49, United States Code, and the item relating to such section in the analysis for chapter 449 of such title.

SEC. 932. CONSOLIDATION OF REPORTS.

(a) Section 44938 of title 49, United States Code is amended—

(1) in the section heading by striking "**Reports**" and inserting "**Transportation security report**";

(2) by striking "(a) TRANSPORTATION SECURITY.—";

(3) by striking the second sentence of subsection (a); and

(4) by striking "and" at the end of subsection (a)(9);

(5) by striking the period at the end of subsection (a)(10) and inserting a semicolon; and

(6) by adding at the end of subsection (a) the following:

"(11) an assessment of the effectiveness of procedures under section 44901;

"(12) a summary of the assessments conducted under section 44907(a)(1) and (2); and

"(13) an assessment of the steps being taken, and the progress being made, in ensuring compliance with section 44906 for each foreign air carrier security program at airports outside the United States—

"(A) at which the Secretary decides that foreign security liaison officers are necessary for air transportation security; and

"(B) for which extraordinary security measures are in place."; and

(7) by striking subsection (b).

(b) The analysis for subchapter II of chapter 449 of such title is amended by striking the item relating to section 44938 and inserting the following:

"44938. Transportation security report.".

SEC. 933. AIRCRAFT CHARTER CUSTOMER AND LESSEE PRESCREENING.

Section 44903(j)(2)(E) of title 49, United States Code, is amended by inserting "certificated" after "maximum" each place it appears.

TITLE X—MISCELLANEOUS PROVISIONS

SEC. 1001. PROTECTION OF DEPARTMENT OF HOMELAND SECURITY NAME, INITIALS, INSIGNIA, AND SEAL.

Section 875 of the Homeland Security Act of 2002 (6 U.S.C. 455) is amended by adding at the end the following new subsection:

"(d) PROTECTION OF NAME, INITIALS, INSIGNIA, AND SEAL.—

"(1) IN GENERAL.—Except with the written permission of the Secretary, no person may knowingly use, in connection with any advertisement, commercial activity, audiovisual production (including film or television production), impersonation, Internet domain name, Internet e-mail address, or Internet web site, merchandise, retail product, or solicitation in a manner reasonably calculated to convey the impression that the Department or any organizational element of the Department has approved, endorsed, or authorized such use, any of the following (or any colorable imitation thereof):

"(A) The words 'Department of Homeland Security', the initials 'DHS', the insignia or seal of the Department, or the title 'Secretary of Homeland Security'.

"(B) The name, initials, insignia, or seal of any organizational element (including any former such element) of the Department, or the title of any other officer or employee of the Department, notice of which has been published by the Secretary of Homeland Security in accordance with paragraph (3).

"(2) CIVIL ACTION.—Whenever it appears to the Attorney General that any person is engaged or is about to engage in an act or practice that constitutes or will constitute conduct prohibited by subsection (d)(1), the Attorney General may initiate a civil proceeding in a district court of the United States to enjoin such act or practice. Such court shall proceed as soon as practicable to the hear-

ing and determination of such action and may, at any time before final determination, enter such restraining orders or prohibitions, or take such other actions as is warranted, to prevent injury to the United States or to any person or class of persons for whose protection the action is brought.

"(3) NOTICE AND PUBLICATION.—The notice and publication to which paragraph (1)(B) refers is a notice published in the Federal Register including the name, initials, seal, or class of titles protected under paragraph (1)(B) and a statement that they are protected under that provision. The Secretary may amend such notices from time to time as the Secretary determines appropriate in the public interest and shall publish such amendments in the Federal Register.

"(4) AUDIOVISUAL PRODUCTION.—For the purpose of this subsection, the term 'audiovisual production' means the production of a work that consists of a series of related images that are intrinsically intended to be shown by the use of machines or devices such as projectors, viewers, or electronic equipment, together with accompanying sounds, if any, regardless of the nature of the material objects, such as films or tapes, in which the work is embodied.".

SEC. 1002. AUTHORIZED USE OF SURPLUS MILITARY VEHICLES.

The Secretary shall include United States military surplus vehicles having demonstrated utility for responding to acts of terrorism, emergencies, and other disasters on the Authorized Equipment List in order to allow states and localities to purchase, modify, upgrade, and maintain such vehicles using homeland security assistance administered by the Department.

SEC. 1003. ENCOURAGING USE OF COMPUTERIZED TRAINING AIDS.

The Under Secretary for Science and Technology shall use and make available to State and local agencies computer simulations to help strengthen the ability of municipalities to prepare for and respond to a chemical, biological, or other terrorist attack, and to standardize response training.

SEC. 1004. EMERGENCY NOTIFICATION SYSTEM STUDY DEADLINE.

Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress the final report on the nationwide emergency notification system study that was prescribed in section 7403 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458).

SEC. 1005. REPORT ON FRAUD PREVENTION EXERCISES.

Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security, working in coordination with the Department of Homeland Security official with primary responsibility for grants and training, shall submit to Congress a report on the feasibility of devising an exercise program to test and evaluate the capabilities of Federal, State, local, and tribal governments to detect and prevent fraud, waste, and abuse in Federal assistance programs administered in response to acts of terrorism, natural disasters, and other emergencies.

SEC. 1006. LIMITATION ON REIMBURSEMENTS RELATING TO CERTAIN DETAILEES.

In the case of an individual assigned to the Department of Homeland Security as a detailee under an arrangement described in subchapter VI of chapter 33 of title 5, United States Code, the maximum reimbursement which may be made under section 3374(c) of such title with respect to such individual for the period of the assignment (including for any employee benefits) may not exceed the total amount of basic pay that would have been payable for such period if such individual had been paid, at the highest rate allowable under section 5382 of such title, as a member of the Senior Executive Service.

PURPOSE AND SUMMARY

The purpose of H.R. 5814 is to authorize appropriations for the Department of Homeland Security, and for other purposes.

BACKGROUND AND NEED FOR LEGISLATION

The Department of Homeland Security (DHS or Department) has been in operation for more than three years. During this time, the Department has experienced a variety of growing pains as it continues to develop, adjust, and integrate various components to achieve its primary missions of preventing terrorist attacks within the United States, reducing our vulnerability to terrorism, and re-

sponding to and recovering from terrorist attacks, if and when they occur.

The complexity of the Department's mission, coupled with the enormity of its management and operational challenges, requires the close and continuing oversight that annual Congressional re-authorization provides. Like the Department of Defense and the Intelligence Community agencies, DHS is—first and foremost—a national security agency. And like those other national security agencies, DHS should be subject to an annual authorization process through which the evolving needs of the Department can be met, and through which Congressional direction, oversight, and prioritization can take place. An annual authorization will help the Department improve the overall management and integration of its various legacy agencies, guide resource allocation and prioritization, set clear and achievable benchmarks for progress and success, and enhance the Department's implementation of its critical mission.

H.R. 5814 is the second DHS authorization bill to be reported by this Committee to the House since the creation of the Department. It builds upon the groundwork laid by the House passage of H.R. 1817, the Department of Homeland Security Authorization Act for 2006. H.R. 5814 is not intended as a comprehensive re-authorization of the Department. Several subjects, including border security, port security, and emergency management reforms have been addressed through separate legislation. The intent of this bill is to make targeted improvements to Department operations, particularly in the area of management and the overall structure of DHS. H.R. 5814 accomplishes these goals within a realistic budgetary framework, consistent with H.R. 5441, the Department of Homeland Security Appropriations Act for Fiscal Year 2007.

HEARINGS

No specific Committee legislative hearings were held on H.R. 5814. However, this authorization bill reflects the findings of numerous oversight hearings that have taken place since passage of the first bill re-authorizing the Department of Homeland Security, H.R. 1817.

On July 14 and July 25, 2005, the Committee held a hearing entitled "The Secretary's Second-Stage Review: Re-thinking the Department of Homeland Security's Organization and Policy Direction." The Committee received testimony from The Honorable Michael Chertoff, Secretary, Department of Homeland Security.

On July 12, 2005, the Subcommittee on Emergency Preparedness, Science, and Technology held a hearing entitled "Project BioShield: Linking Bioterrorism Threats and Countermeasure Procurement to Enhance Terrorism Preparedness." The Subcommittee received testimony from The Honorable Stewart Simonson, Assistant Secretary, Office of Public Health Emergency Preparedness, Department of Health and Human Services; Dr. John Vitko, Jr., Director, Biological Countermeasures Portfolio, Directorate of Science and Technology, Department of Homeland Security; Ms. Karen T. Morr, Acting Assistant Secretary, Office of Information Analysis, Information Analysis and Infrastructure Protection Directorate, Department of Homeland Security; Dr. Marcus Eugene Carr, Jr., Executive Director, Clinical Research—Hemostasis, Novo

Nordisk, Inc.; Mr. Michael Greenberger, Director, Center for Health and Homeland Security, University of Maryland School of Law; Mr. Richard Hollis, Chief Executive Officer, Hollis-Eden Pharmaceuticals, Inc.; Mr. James A. Joyce, Chairman and Chief Executive Officer, Aethlon Medical, Inc.; Mr. David P. Wright, President and Chief Executive Officer, PharmAthene, Inc.; and Ms. Nancy Wysenski, President, EMD Pharmaceuticals.

On September 28, 2005, the Subcommittee on Management, Integration, and Oversight received a Member briefing and demonstration on canine units. The Committee also held a hearing entitled "Sniffing Out Terrorism: The Use of Dogs in Homeland Security." The Subcommittee received testimony from Mr. Lee Titus, Director of Canine Programs, U.S. Customs and Border Protection, Department of Homeland Security; Mr. David Kontny, Director, National Explosives Detection Canine Team Program, Transportation Security Administration, Department of Homeland Security; Special Agent Terry Bohan, Chief, National Canine Training and Operations Support Branch, Bureau of Alcohol, Tobacco, Firearms and Explosives, Department of Justice; Chief Ralph Eugene Wilson, Jr., Chief of Police, Metropolitan Atlanta Rapid Transit Authority (MARTA); Dr. C. Michael Moriarty, Associate Provost and Vice President for Research, Auburn University; and Ms. Terri Recknor, President, Garrison and Sloan Canine Detection.

On October 18, 2005, the Subcommittee on Emergency Preparedness, Science, and Technology and the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity held a joint hearing entitled "SCADA and the Terrorist Threat: Protecting the Nation's Critical Control Systems." The Subcommittees received testimony from Mr. Donald "Andy" Purdy, Acting Director, National Cyber Security Division, U.S. Department of Homeland Security; Mr. Larry Todd, Director, Security, Safety and Law Enforcement, Bureau of Reclamation, U.S. Department of the Interior; Dr. Sam Varnado, Director of Information Operations Center, Sandia National Laboratory; Dr. K.P. Ananth, Associate Laboratory Director, National & Homeland Security, Idaho National Laboratory; Dr. William Rush, Institute Physicist, Gas Technology Institute; and Mr. Alan Paller, Director of Research, The SANS Institute.

On October 27, 2005, the Subcommittee on Management, Integration, and Oversight held a hearing entitled "The Department of Homeland Security Second-Stage Review: The Role of the Chief Medical Officer." Testimony was received from Dr. Jeffrey W. Runge, Chief Medical Officer, Department of Homeland Security; Mr. Timothy Moore, Director of Federal Programs, National Agricultural Biosecurity Center, Kansas State University; Dr. Jeffrey A. Lowell, Professor of Surgery and Pediatrics, Washington University School of Medicine; and Mr. David Heyman, Director and Senior Fellow, Homeland Security Program, Center for Strategic and International Studies.

On February 15, 2006, the Committee on Homeland Security held a hearing entitled "The President's Fiscal Year 2007 Budget for the Department of Homeland Security: Maintaining Vigilance and Improving Mission Performance in Securing the Homeland." The Committee received testimony from The Honorable Michael Chertoff, Secretary, Department of Homeland Security.

On February 15, 2006, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity held a hearing entitled "The President's Fiscal Year 2007 Budget: Coast Guard Programs Impacting Maritime Border Security." The Subcommittee received testimony from Admiral Thomas H. Collins, Commandant, U.S. Coast Guard.

On February 8, 2006, the Subcommittee on Emergency Preparedness, Science, and Technology and the Subcommittee on Prevention of Nuclear and Biological Attack held a joint hearing entitled "Protecting the Homeland: Fighting Pandemic Flu From the Front Lines." The Subcommittees received testimony from Dr. Tara O'Toole, Chief Executive Officer and Director, Center for Biosecurity, University of Pittsburgh Medical Center; The Honorable David B. Mitchell, Secretary, Department of Safety and Homeland Security, State of Delaware; Ms. Frances B. Phillips, RN, MHA, Health Officer, Anne Arundel County, Maryland Department of Health; Mr. Ernest Blackwelder, Senior Vice President, Business Force, Business Executives for National Security; and Dr. David C. Seaberg, Department of Emergency Medicine, University of Florida.

On March 29, 2006, the Subcommittee on Management, Integration, and Oversight of the Committee on Homeland Security and the Subcommittee on Government Management, Finance, and Accountability of the Committee on Government Reform held a joint hearing entitled "Department of Homeland Security Information Technology Challenges and the Future of eMerge2." The Subcommittees received testimony from Mr. McCoy Williams, Director, Financial Management and Assurance, Government Accountability Office; Mr. Randy Hite, Director, Information Technology Architecture and Systems, Government Accountability Office; Mr. Eugene Schied, Acting Chief Financial Officer, Department of Homeland Security; and Mr. Scott Charbo, Chief Information Officer, Department of Homeland Security.

On May 16, 2006, the Committee on Homeland Security held a hearing entitled "Are We Ready?: Implementing the National Strategy for Pandemic Influenza." The Committee received testimony from The Honorable Jeffrey W. Runge, Acting Undersecretary, Science and Technology, and Chief Medical Officer, Department of Homeland Security; The Honorable John Agwonobi, Assistant Secretary for Health, Department of Health and Human Services; The Honorable John Clifford, Deputy Administrator for Veterinary Services, Animal and Plant Health Inspection Service, Department of Agriculture; and The Honorable Peter F. Verga, Deputy Assistant Secretary of Defense for Homeland Defense, Department of Defense.

On May 18, 2006, the Subcommittee on Management, Integration, and Oversight held a hearing entitled "Retention, Security Clearances, Morale, and Other Human Capital Challenges Facing the Department of Homeland Security." The Subcommittee received testimony from Mr. K. Gregg Prillaman, Chief Human Capital Officer, U.S. Department of Homeland Security; Mr. Dwight Williams, Director, Office of Security, U.S. Department of Homeland Security; Ms. Kathy L. Dillaman, Associate Director, Federal Investigations Processing Center, U.S. Office of Personnel Management; Mr. John Gage, National President, American Federation of

Government Employees; Ms. Colleen M. Kelley, President, National Treasury Employees Union; and Professor Charles Tiefer, Professor of Law, University of Baltimore School of Law.

COMMITTEE CONSIDERATION

H.R. 5814 was introduced by Mr. King of New York, Mr. Thompson of Mississippi, Mr. Rogers of Alabama, and Mr. Meek of Florida on July 17, 2006, and referred solely to the Committee on Homeland Security.

On July 19, 2006, the Full Committee met in open markup session and ordered H.R. 5814 reported to the House, amended, by voice vote.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto.

On July 19, 2006, the Full Committee met in open markup session and ordered H.R. 5814 reported to the House, amended, by voice vote.

The following actions occurred:

H.R. 5814, to authorize appropriations for the Department of Homeland Security, and for other purposes; was AGREED TO, amended, by a record vote of 30 yeas and 1 nay. (Rollcall Vote No. 45).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Wednesday, July 19, 2006 Convened: 10:10 a.m.

Adjourned: 2:05 p.m.

Meeting on : Markup of H.R. 5814, to authorize appropriations for the Department of Homeland Security, and for other purposes. On agreeing to H.R. 5814, as amended.

☐ Attendance ☒ Recorded Vote Vote Number: 45 Total: Yeas 30 Nays 1

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska	✓			*Mr. Bennie G. Thompson* *Mississippi, Ranking Member*	✓		
Mr. Lamar S. Smith Texas	✓			*Ms. Loretta Sanchez* *California*	✓		
Mr. Curt Weldon Pennsylvania	✓			*Mr. Edward J. Markey* *Massachusetts*		✓	
Mr. Christopher Shays Connecticut	✓			*Mr. Norman D. Dicks* *Washington*	✓		
Mr. John Linder Georgia	✓			*Ms. Jane Harman* *California*	✓		
Mr. Mark E. Souder Indiana	✓			*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Tom Davis Virginia	✓			*Ms. Nita M. Lowey* *New York*	✓		
Mr. Daniel E. Lungren California	✓			*Ms. Eleanor Holmes Norton* *District of Columbia*	✓		
Mr. Jim Gibbons Nevada	✓			*Ms. Zoe Lofgren* *California*	✓		
Mr. Rob Simmons Connecticut	✓			*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Mike Rogers Alabama	✓			*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Stevan Pearce New Mexico	✓			*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Ms. Katherine Harris Florida				*Mr. Bob Etheridge* *North Carolina*	✓		
Mr. Bobby Jindal Louisiana				*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Dave Reichert Washington	✓			*Mr. Kendrick Meek* *Florida*	✓		
Mr. Michael McCaul Texas	✓						
Mr. Charlie Dent Pennsylvania	✓						
Ms. Ginny Brown-Waite Florida	✓						
Mr. Peter T. King New York Chairman	✓			Total	**30**	**1**	

The following amendments were offered:

An Amendment in the Nature of a Substitute (#1) offered by Mr. King; was AGREED TO, as amended, by voice vote.

A unanimous consent request by Mr. King to consider the Amendment in the Nature of a Substitute as base text for purposes of amendment, was not objected to.

An amendment offered by Mr. Thompson to the Amendment in the Nature of a Substitute offered by Mr. King (#1A); in section 101, strike the dollar amount and insert "$40,850,134,400".; was NOT AGREED TO by a record vote of 13 yeas and 16 nays (Rollcall Vote No. 38).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Wednesday, July 19, 2006 Convened: 10:10 a.m.

Adjourned: 2:05 p.m.

Meeting on : Markup of H.R. 5814, to authorize appropriations for the Department of Homeland Security, and for other purposes. On agreeing to amendment #1A offered by Mr. Thompson

☐ Attendance ☒ Recorded Vote Vote Number: 38 Total: Yeas 13 Nays 16

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska				*Mr. Bennie G. Thompson* *Mississippi, Ranking Member*	✓		
Mr. Lamar S. Smith Texas		✓		*Ms. Loretta Sanchez* *California*	✓		
Mr. Curt Weldon Pennsylvania		✓		*Mr. Edward J. Markey* *Massachusetts*	✓		
Mr. Christopher Shays Connecticut		✓		*Mr. Norman D. Dicks* *Washington*	✓		
Mr. John Linder Georgia		✓		*Ms. Jane Harman* *California*	✓		
Mr. Mark E. Souder Indiana		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Tom Davis Virginia		✓		*Ms. Nita M. Lowey* *New York*	✓		
Mr. Daniel E. Lungren California		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*			
Mr. Jim Gibbons Nevada		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Rob Simmons Connecticut		✓		*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Mike Rogers Alabama		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Ms. Katherine Harris Florida				*Mr. Bob Etheridge* *North Carolina*	✓		
Mr. Bobby Jindal Louisiana				*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Dave Reichert Washington		✓		*Mr. Kendrick Meek* *Florida*	✓		
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Ms. Ginny Brown-Waite Florida		✓					
Mr. Peter T. King New York Chairman		✓		Total	**13**	**16**	

An amendment offered by Ms. Sanchez to the Amendment in the Nature of a Substitute offered by Mr. King (#1B); in subtitle A of section II, add a new section entitled "Sec. 206. Offices."; was WITHDRAWN by unanimous consent.

An amendment offered by Mr. Pascrell to the Amendment in the Nature of a Substitute offered by Mr. King (#1C); at the appropriate place in the bill, insert a new section entitled "Sec. ____. Certification Requirements for Offerors for Department of Homeland Security Contracts."; was AGREED TO by voice vote.

An amendment offered by Mrs. Christensen to the Amendment in the Nature of a Substitute offered by Mr. King (#1D); insert at the appropriate place a new title "Title ____—Priority Countermeasures Against Pathogens and Toxins."; was WITHDRAWN by unanimous consent.

An amendment offered by Mrs. Lowey to the Amendment in the Nature of a Substitute offered by Mr. King (#1E); at the end of title VII insert a new section entitled "Sec. ____. National Asset Database."; was AGREED TO by voice vote.

An amendment offered by Mr. Langevin to the Amendment in the Nature of a Substitute offered by Mr. King (#1F); at the appropriate place in the bill, insert a new section entitled "Sec. ____. Authorization of Appropriations."; was NOT AGREED TO by a record vote of 13 yeas and 16 nays (Rollcall Vote No. 40).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Wednesday, July 19, 2006 Convened: 10:10 a.m.
Adjourned: 2:05 p.m.

Meeting on : Markup of H.R. 5814, to authorize appropriations for the Department of Homeland Security, and for other purposes. On agreeing amendment #1F by Mr. Langevin

☐ Attendance ☒ Recorded Vote Vote Number: 40 Total: Yeas 13 Nays 16

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska				*Mr. Bennie G. Thompson* *Mississippi, Ranking Member*	✓		
Mr. Lamar S. Smith Texas		✓		*Ms. Loretta Sanchez* *California*	✓		
Mr. Curt Weldon Pennsylvania		✓		*Mr. Edward J. Markey* *Massachusetts*	✓		
Mr. Christopher Shays Connecticut		✓		*Mr. Norman D. Dicks* *Washington*	✓		
Mr. John Linder Georgia		✓		*Ms. Jane Harman* *California*	✓		
Mr. Mark E. Souder Indiana		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Tom Davis Virginia		✓		*Ms. Nita M. Lowey* *New York*	✓		
Mr. Daniel E. Lungren California		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*			
Mr. Jim Gibbons Nevada		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Rob Simmons Connecticut		✓		*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Mike Rogers Alabama		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Ms. Katherine Harris Florida				*Mr. Bob Etheridge* *North Carolina*	✓		
Mr. Bobby Jindal Louisiana				*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Dave Reichert Washington		✓		*Mr. Kendrick Meek* *Florida*	✓		
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Ms. Ginny Brown-Waite Florida		✓					
Mr. Peter T. King New York Chairman		✓		Total	**13**	**16**	

An amendment offered by Ms. Sanchez to the Amendment in the Nature of a Substitute offered by Mr. King (#1G); in section 901(a), in the proposed section 481, strike subsections (e) and (f), redesignate subsection (g) as subsection (k), and insert at the end of subsection (d) a new section "(3) Review of Security Plans."; and in section 903, in the proposed section 802, strike subsections (c), (d), and (e) and insert a new section "(c) Requires Programs."; was WITHDRAWN by unanimous consent.

An amendment offered by Mrs. Lowey to the Amendment in the Nature of a Substitute offered by Mr. King (#1H); insert at the appropriate place a new section entitled "Sec. ____. Provisions relating to TSA Personnel Management."; was NOT AGREED TO by a record vote of 14 yeas and 15 nays (Rollcall Vote No. 41).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Wednesday, July 19, 2006 Convened: 10:10 a.m.

Adjourned: 2:05 p.m.

Meeting on : Markup of H.R. 5814, to authorize appropriations for the Department of Homeland Security, and for other purposes. On agreeing amendment #1H by Mrs. Lowey

☐ Attendance ☒ Recorded Vote Vote Number: 41 Total: Yeas 14 Nays 15

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska				*Mr. Bennie G. Thompson* *Mississippi, Ranking Member*	✓		
Mr. Lamar S. Smith Texas		✓		*Ms. Loretta Sanchez* *California*	✓		
Mr. Curt Weldon Pennsylvania		✓		*Mr. Edward J. Markey* *Massachusetts*	✓		
Mr. Christopher Shays Connecticut		✓		*Mr. Norman D. Dicks* *Washington*	✓		
Mr. John Linder Georgia		✓		*Ms. Jane Harman* *California*	✓		
Mr. Mark E. Souder Indiana		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Tom Davis Virginia		✓		*Ms. Nita M. Lowey* *New York*	✓		
Mr. Daniel E. Lungren California		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*			
Mr. Jim Gibbons Nevada		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Rob Simmons Connecticut	✓			*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Mike Rogers Alabama		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Ms. Katherine Harris Florida				*Mr. Bob Etheridge* *North Carolina*	✓		
Mr. Bobby Jindal Louisiana				*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Dave Reichert Washington		✓		*Mr. Kendrick Meek* *Florida*	✓		
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Ms. Ginny Brown-Waite Florida		✓					
Mr. Peter T. King New York Chairman		✓		Total	**14**	**15**	

An amendment offered by Mr. Markey to the Amendment in the Nature of a Substitute offered by Mr. King (#1I); at the appropriate place in the bill, insert a new section entitled "Sec. ____. Inspection of Cargo Carried Aboard Passenger Aircraft."; was NOT AGREED TO by a record vote of 14 yeas and 15 nays (Rollcall Vote No. 42).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Wednesday, July 19, 2006 Convened: 10:10 a.m.

Adjourned: 2:05 p.m.

Meeting on : Markup of H.R. 5814, to authorize appropriations for the Department of Homeland Security, and for other purposes. On agreeing amendment #11 by Mr. Markey

☐ Attendance ☒ Recorded Vote Vote Number: 42 Total: Yeas 14 Nays 15

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska				*Mr. Bennie G. Thompson* *Mississippi, Ranking Member*	✓		
Mr. Lamar S. Smith Texas		✓		*Ms. Loretta Sanchez* *California*	✓		
Mr. Curt Weldon Pennsylvania		✓		*Mr. Edward J. Markey* *Massachusetts*	✓		
Mr. Christopher Shays Connecticut	✓			*Mr. Norman D. Dicks* *Washington*	✓		
Mr. John Linder Georgia		✓		*Ms. Jane Harman* *California*	✓		
Mr. Mark E. Souder Indiana		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Tom Davis Virginia		✓		*Ms. Nita M. Lowey* *New York*	✓		
Mr. Daniel E. Lungren California		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*			
Mr. Jim Gibbons Nevada		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Rob Simmons Connecticut		✓		*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Mike Rogers Alabama		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Ms. Katherine Harris Florida				*Mr. Bob Etheridge* *North Carolina*	✓		
Mr. Bobby Jindal Louisiana				*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Dave Reichert Washington		✓		*Mr. Kendrick Meek* *Florida*	✓		
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Ms. Ginny Brown-Waite Florida		✓					
Mr. Peter T. King New York Chairman		✓		Total	**14**	**15**	

An amendment offered by Ms. Jackson-Lee to the Amendment in the Nature of a Substitute offered by Mr. King (#1J); insert at the appropriate place the following new section entitled "Sec. ____. Highest Grade Allowable for Certain Border Patrol Agent or Officer Positions."; was NOT AGREED TO by a record vote of 13 yeas and 16 nays (Rollcall Vote No. 39).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Wednesday, July 19, 2006 Convened: 10:10 a.m.

Adjourned: 2:05 p.m.

Meeting on : Markup of H.R. 5814, to authorize appropriations for the Department of Homeland Security, and for other purposes. On agreeing amendment #1J by Ms. Jackson-Lee

☐ Attendance ☒ Recorded Vote Vote Number: 39 Total: Yeas 13 Nays 16

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska				*Mr. Bennie G. Thompson* *Mississippi, Ranking Member*	✓		
Mr. Lamar S. Smith Texas		✓		*Ms. Loretta Sanchez* *California*	✓		
Mr. Curt Weldon Pennsylvania		✓		*Mr. Edward J. Markey* *Massachusetts*	✓		
Mr. Christopher Shays Connecticut		✓		*Mr. Norman D. Dicks* *Washington*	✓		
Mr. John Linder Georgia		✓		*Ms. Jane Harman* *California*	✓		
Mr. Mark E. Souder Indiana		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Tom Davis Virginia		✓		*Ms. Nita M. Lowey* *New York*	✓		
Mr. Daniel E. Lungren California		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*			
Mr. Jim Gibbons Nevada		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Rob Simmons Connecticut		✓		*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Mike Rogers Alabama		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Ms. Katherine Harris Florida				*Mr. Bob Etheridge* *North Carolina*	✓		
Mr. Bobby Jindal Louisiana				*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Dave Reichert Washington		✓		*Mr. Kendrick Meek* *Florida*	✓		
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Ms. Ginny Brown-Waite Florida		✓					
Mr. Peter T. King New York Chairman		✓		Total	**13**	**16**	

An amendment offered by Ms. Jackson-Lee to the Amendment in the Nature of a Substitute offered by Mr. King (#1K); at the end of title II, insert a new section entitled "Sec. 3 ____. TSA Acquisition Management Policy."; was WITHDRAWN by unanimous consent.

An amendment offered by Ms. Jackson-Lee to the Amendment in the Nature of a Substitute offered by Mr. King (#1L); insert at the appropriate place a new section entitled "Sec. ____. Contracts for Assistance Activities Relating to Act of Terrorism, Natural Disasters, and Other Emergencies."; was AGREED TO by voice vote.

An amendment offered by Mr. Markey to the Amendment in the Nature of a Substitute offered by Mr. King (#1M); at the end of the bill, insert a new section entitled "Sec. ____. Discrimination against Whistleblowers Prohibited."; was NOT AGREED TO by a record vote of 14 yeas and 16 nays (Rollcall Vote No. 43).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Wednesday, July 19, 2006 Convened: 10:10 a.m.

Adjourned: 2:05 p.m.

Meeting on : Markup of H.R. 5814, to authorize appropriations for the Department of Homeland Security, and for other purposes. On agreeing amendment #1M by Mr. Markey

☐ Attendance ☒ Recorded Vote Vote Number: 43 Total: Yeas 14 Nays 16

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska				*Mr. Bennie G. Thompson* *Mississippi, Ranking Member*	✓		
Mr. Lamar S. Smith Texas		✓		*Ms. Loretta Sanchez* *California*	✓		
Mr. Curt Weldon Pennsylvania		✓		*Mr. Edward J. Markey* *Massachusetts*	✓		
Mr. Christopher Shays Connecticut		✓		*Mr. Norman D. Dicks* *Washington*	✓		
Mr. John Linder Georgia		✓		*Ms. Jane Harman* *California*	✓		
Mr. Mark E. Souder Indiana		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Tom Davis Virginia		✓		*Ms. Nita M. Lowey* *New York*	✓		
Mr. Daniel E. Lungren California		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*	✓		
Mr. Jim Gibbons Nevada		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Rob Simmons Connecticut		✓		*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Mike Rogers Alabama		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Ms. Katherine Harris Florida				*Mr. Bob Etheridge* *North Carolina*	✓		
Mr. Bobby Jindal Louisiana				*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Dave Reichert Washington		✓		*Mr. Kendrick Meek* *Florida*	✓		
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Ms. Ginny Brown-Waite Florida		✓					
Mr. Peter T. King New York Chairman		✓		Total	**14**	**16**	

An amendment offered by Ms. Norton to the Amendment in the Nature of a Substitute offered by Mr. King (#1N); insert at the appropriate place a new section entitled "Repeal of Authority to Establish Human Resources Management System."; was NOT AGREED TO by a record vote of 14 yeas and 17 nays (Rollcall Vote No. 44).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Wednesday, July 19, 2006 Convened: 10:10 a.m.

Adjourned: 2:05 p.m.

Meeting on : Markup of H.R. 5814, to authorize appropriations for the Department of Homeland Security, and for other purposes. On agreeing amendment #1N by Ms. Norton

☐ Attendance ☒ Recorded Vote Vote Number: 44 Total: Yeas 14 Nays 17

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska		✓		*Mr. Bennie G. Thompson* *Mississippi, Ranking Member*	✓		
Mr. Lamar S. Smith Texas		✓		*Ms. Loretta Sanchez* *California*	✓		
Mr. Curt Weldon Pennsylvania		✓		*Mr. Edward J. Markey* *Massachusetts*	✓		
Mr. Christopher Shays Connecticut		✓		*Mr. Norman D. Dicks* *Washington*	✓		
Mr. John Linder Georgia		✓		*Ms. Jane Harman* *California*	✓		
Mr. Mark E. Souder Indiana		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Tom Davis Virginia		✓		*Ms. Nita M. Lowey* *New York*	✓		
Mr. Daniel E. Lungren California		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*	✓		
Mr. Jim Gibbons Nevada		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Rob Simmons Connecticut		✓		*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Mike Rogers Alabama		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Ms. Katherine Harris Florida				*Mr. Bob Etheridge* *North Carolina*	✓		
Mr. Bobby Jindal Louisiana				*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Dave Reichert Washington		✓		*Mr. Kendrick Meek* *Florida*	✓		
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Ms. Ginny Brown-Waite Florida		✓					
Mr. Peter T. King New York Chairman		✓		Total	**14**	**17**	

An amendment offered by Ms. Sanchez to the Amendment in the Nature of a Substitute offered by Mr. King (#1O); insert at the appropriate place a new section entitled "Sec. ____. Limitation on Reimbursements Relating to Certain Detailees."; was AGREED TO by voice vote.

An amendment offered by Ms. Sanchez to the Amendment in the Nature of a Substitute offered by Mr. King (#1P); at the end of title VII add a new section entitled "Sec. ____. Metropolitan Medical Response System."; was AGREED TO by voice vote.

An amendment offered by Mr. Markey to the Amendment in the Nature of a Substitute offered by Mr. King (#1Q); insert at the appropriate section of the bill a section relating to the issuance and guidance of purchase cards; was AGREED TO by voice vote.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

The purpose of H.R. 5814, Department of Homeland Security Authorization Act for Fiscal Year 2007 is provide for the authorization and guidance for the Department of Homeland Security and its authorities.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 5814, Department of Homeland Security Authorization Act for Fiscal Year 2007, would result in no significant new or increased budget authority, entitlement authority, or tax expenditures or revenues.

The Committee notes that Section 916 of H.R. 5814, authorizes the Transportation Security Administration (TSA) to charge a fee to perform background checks on non-U.S. citizens seeking training at United States flight schools, which would result in some new revenues. However, the Congressional Budget Office (CBO) estimates, based on information from TSA about the increased number of background checks the agency would perform under the bill, that additional receipts would total about $1.5 million annually. Because TSA has permanent authority to spend such receipts, CBO estimates that any such increases would be offset by corresponding increases in direct spending of about the same amount. Therefore, any net change in direct spending under the bill would not be significant in any given year.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 17, 2006.

Hon. PETER T. KING,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has completed the enclosed cost estimate for H.R. 5814, the Department of Homeland Security Authorization Act for Fiscal Year 2007.

The CBO staff contacts for this estimate are Mark Grabowicz (for federal costs), Melissa Merrell (for the impact on state and local governments), and Paige Piper/Bach (for the impact on the private sector).

Sincerely,

DONALD B. MARRON,
Acting Director.

Enclosure.

H.R. 5814—Department of Homeland Security Authorization Act for Fiscal Year 2007

Summary: Public Law 109–295, the Department of Homeland Security Appropriations Act for 2007, provided $33.7 billion to the Department of Homeland Security (DHS) for 2007 operations. CBO estimates that H.R. 5814 would authorize the appropriation of $34.8 billion for fiscal year 2007 to fund DHS operations—about $1 billion more than the amount appropriated thus far in 2007.

In addition, CBO estimates that the bill would authorize the appropriation of nearly $10 billion for the Transportation Security Administration (TSA) and a few other programs within DHS over the 2008–2012 period. CBO estimates that implementing H.R. 5814 would result in new discretionary spending of $10.4 billion over the 2007–2012 period in addition to the amounts already appropriated to DHS for 2007.

CBO also estimates that enacting a provision to authorize TSA to charge fees to non-U.S. citizens seeking recurrent training at flight schools would slightly increase both offsetting receipts and subsequent direct spending of those receipts. We estimate that any resulting net change in direct spending would not be significant in any year. Enacting H.R. 5814 would not affect revenues.

H.R. 5814 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA) because it would require certain public transportation agencies to conduct vulnerability assessments and to create and implement security plans. While CBO cannot estimate the aggregate costs of these mandates, based on information from industry and government sources, we estimate that the costs to state, local, and tribal governments would exceed the threshold ($64 million in 2006, adjusted annually for inflation) in at least one of the first five years after enactment. The bill would authorize appropriations of funds to cover those costs.

Other provisions of the bill would change how certain DHS grants for first responders are allocated to states and localities. Some states would receive less funding than in previous years,

while others would receive more. On balance, state, local, and tribal governments would benefit from the provisions in this bill.

H.R. 5814 would impose several private-sector mandates, as defined in UMRA, on rail carriers, transportation systems, and certain individuals. CBO estimates that the direct cost of complying with most of those mandates would be small and fall well below the annual threshold for private-sector mandates established by UMRA ($128 million in 2006, adjusted annually for inflation). However, because the cost of one of the mandates would depend on regulations that have not yet been issued, CBO cannot determine whether the aggregate cost of all the private-sector mandates in the bill would exceed the annual threshold.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 5814 is shown in the following table. The costs of this legislation fall within budget functions 050 (national defense), 300 (natural resources and environment), 400 (transportation), 450 (community and regional development), 550 (health), 600 (income security), 750 (administration of justice), and 800 (general government).

Basis of estimate: CBO estimates that implementing H.R. 5814 would cost an additional $10.4 billion over the 2007–2012 period relative to the amount already appropriated to DHS for 2007, assuming appropriation of the amounts authorized and estimated to be necessary. For this estimate, we assume that the necessary amounts will be appropriated each year. Estimated outlays are based on historical spending patterns for existing or similar programs. In addition, CBO estimates that the bill would have an insignificant effect on direct spending.

	By fiscal year, in millions of dollars—					
	2007	2008	2009	2010	2011	2012
SPENDING SUBJECT TO APPROPRIATION						
DHS Spending Under Current Law:						
Estimated Budget Authority[1]	33,734	0	0	0	0	0
Estimated Outlays	43,578	7,598	3,597	1,368	358	172
Proposed Changes:						
Major DHS Programs:						
Authorization Level[2]	964	0	0	0	0	0
Estimated Outlays	492	212	145	67	29	15
ODND:						
Estimated Authorization Level	0	547	558	569	580	592
Estimated Outlays	0	273	443	561	572	584
Net Funding for Aviation Security:						
Estimated Authorization Level	0	2,155	2,205	2,299	0	0
Estimated Outlays	0	1,422	2,181	2,274	781	0
Other Transportation Security Activities:						
Estimated Authorization Level	53	51	51	51	51	
Estimated Outlays	46	51	51	51	51	51
Other DHS Programs:						
Estimated Authorization Level	13	23	24	3	3	0
Estimated Outlays	9	22	23	5	3	2
Total Changes:						
Estimated Authorization Level	1,030	2,776	2,837	2,922	634	643
Estimated Outlays	546	1,980	2,843	2,959	1,436	652
Spending Under H.R. 5814:						
Estimated Authorization Level	34,764	2,776	2,837	2,922	634	643
Estimated Outlays	44,124	9,578	6,440	4,327	1,794	824

[1] The estimated 2007 level is the amount of appropriations less offsetting collections for that year for operations of DHS.

[2] The amount shown is the difference between H.R. 5814's gross authorization level for 2007 and the amount already appropriated for that year.

Note.—ODND = Office of Defense Nuclear Detection.

Spending subject to appropriation

H.R. 5814 would authorize appropriations for major DHS programs in 2007. It also would authorize additional appropriations in 2007 and later years for programs related to domestic nuclear detection, transportation security, and other activities.

Major DHS Programs. Section 101 of H.R. 5814 would authorize the appropriation of $34.8 billion for fiscal year 2007 to fund the major operations of DHS other than the Transportation Security Agency's aviation security programs, which are funded in title IX of the bill. The bill would not authorize any appropriation after 2007 for these activities. Public Law 109–295, the Department of Homeland Security Appropriation Act for 2007, provided $33.7 billion for DHS for 2007; thus, H.R. 5814 would authorize the appropriation of about $1 billion more in 2007 for major DHS operations.

Office of Defense Nuclear Detection (ODND). Of the amount authorized in section 101 of H.R. 5814, the bill would provide $536 million for ODND and would authorize the appropriation of such sums as may be necessary for each subsequent year for that office. CBO estimated the authorization levels for ODND for fiscal years 2008 through 2011 by adjusting the 2007 level for anticipated annual inflation. Public Law 109–295 provided $481 million for ODND for fiscal year 2007.

Aviation Security. H.R. 5814 would authorize the appropriation of necessary sums for TSA's aviation security programs for fiscal years 2007–2010, particularly for salaries for screeners of passengers and baggage, and for related expenses. For fiscal year 2007, the Congress has already provided net funding of $2.3 billion for TSA's aviation security programs. In addition, TSA also has authority to spend $2.4 billion in fees that we expect the agency will collect this year. For this estimate, we assume that those amounts are sufficient to carry out aviation security activities authorized under H.R. 5814 for 2007.

CBO estimates that, under H.R. 5814, continuing aviation security programs over the 2008–2010 period would require gross appropriations totaling $15.1 billion. That estimate assumes that funding for those activities would remain at 2007 levels, adjusted to keep pace with anticipated inflation in future years.

For this estimate, CBO assumes that a portion of the $15.1 billion authorized for aviation security over the next three years would come from certain fees that TSA is authorized to collect to offset the agency's costs. Most of those collections would result from fees charged on tickets sold by commercial airlines. Additional collections would result from certain fees paid directly to TSA by air carriers. (Under existing law, TSA's authority to collect and spend such fees is subject to appropriation.) Based on information from TSA about anticipated numbers of airline passengers and other key factors, CBO estimates that such fees would offset about $8.4 billion of amounts provided for aviation security over the 2008–2010 period, thus reducing the net level of funding from the U.S. Treasury that would be necessary to implement the bill. Accordingly, we estimate that fully funding aviation security programs under H.R. 5814 would require net appropriations totaling $6.7 billion over the 2008–2010 period (averaging a little more than $2.2 billion a year as shown in the table above).

Other Transportation Security Activities. H.R. 5814 would authorize the appropriation of $50 million a year over the 2007–2010 period and necessary sums thereafter for TSA to research and develop technologies to improve transportation security. The bill also would authorize TSA to complete various other activities, studies, and reports to the Congress. Based on historical spending patterns for similar programs and assuming appropriation of the specified and estimated amounts, CBO estimates that those activities would cost $46 million in 2007 and $301 million over the 2007–2012 period.

Other DHS Programs. H.R. 5814 would authorize the appropriation of $3 million for each of fiscal years 2007 through 2011 for DHS to make grants to U.S. canine breeders to improve the department's canine detection program. The bill also would authorize the appropriation of $10 million for 2007 for the Human Smuggling and Trafficking Center, an interagency program involving DHS, the Department of State, the Department of Justice, and the intelligence community. Finally, H.R. 5814 would authorize the appropriation of sums necessary for fiscal years 2008 and 2009 for DHS to prepare assessments of terrorist threats using chemical, biological, nuclear, and other weapons or agents. Based on information from DHS about the funding provided for threat assessments for fiscal year 2006, CBO estimates that implementing this provision would cost about $20 million annually over the 2008–2009 period.

Direct spending

CBO estimates that enacting H.R. 5814 would increase offsetting receipts from fees charged by TSA to perform background checks on non-U.S. citizens seeking training at U.S. flight schools. Based on information from TSA about the increased number of background checks the agency would perform under the bill, we estimate that additional receipts would total about $1.5 million annually. Because TSA has permanent authority to spend such receipts, we estimate that any such increases would be offset by corresponding increases in direct spending of about the same amount. Therefore, any net change in direct spending under the bill would not be significant in any year.

Estimated impact on state, local, and tribal governments: H.R. 5814 contains intergovernmental mandates as defined in UMRA because it would require certain public transportation agencies to conduct vulnerability assessments and to create and implement security plans. While CBO cannot estimate the aggregate costs of those mandates, based on information from industry and government sources, we estimate that the costs to state, local, and tribal governments would exceed the threshold ($64 million in 2006, adjusted annually for inflation) in at least one of the first five years after enactment. The bill would authorize appropriations of funds to cover those costs.

Mandates on public transit entities

H.R. 5814 would require certain public transportation agencies to conduct vulnerability assessments and to create and implement security plans within two years after enactment of the legislation. The requirements would affect more than 300 public transit entities and ferry systems. Under current law, about one-third of af-

fected agencies have already conducted such assessments and have implemented security plans. They likely would not be required to repeat the process.

More than 200 transit and ferry systems, however, would be required to conduct vulnerability assessments and to create and implement security plans as a result of this bill's enactment. Although the costs to each individual system would likely vary, based on information from industry and government sources, CBO estimates that the aggregate costs to transit and ferry systems likely would exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation) in at least one of the first five years after enactment. The bill would authorize the appropriation of $400 million in fiscal year 2007 to cover these costs.

Other impacts

Other provisions of the bill would make several changes to existing grant programs for state, local, and tribal governments. First, it would change the criteria for at least three current programs—the State Homeland Security Grant, the Law Enforcement Terrorism Prevention Program, and the Urban Area Security Initiative—and change how those funds are allocated. Some states would receive less funding than in previous years, and others would receive more. This bill would allow some local governments to apply for funds directly (rather than receiving them through their states) and would expand eligible activities to include covering the costs of some overtime activities during heightened threat alerts and training activities.

The bill also would authorize DHS to transfer funds directly to the local recipients if states fail to provide funds to local first responders in a timely manner. States would be required to provide at least 80 percent of the funds or resources to local recipients within 45 days of receipt.

On balance, state, local, and tribal governments would benefit from provisions that require DHS to create, with input from local first responders and trade representatives, essential capabilities and voluntary standards for equipment and training.

Estimated impact on the private sector: H.R. 5814 would impose several private-sector mandates, as defined in UMRA, on rail carriers, transportation systems, and certain individuals. CBO estimates that the direct cost of complying with most of those mandates would be small and fall well below the annual threshold for private-sector mandates established by UMRA ($128 million in 2006, adjusted annually for inflation). However, because the cost of one of the mandates would depend on regulations that have not yet been issued, CBO cannot determine whether the aggregate cost of all the private-sector mandates in the bill would exceed the annual threshold.

Vulnerability assessments and security plans

Section 901 would require the Secretary of the Department of Homeland Security to establish by regulation standards, protocols, and procedures for vulnerability assessments and security plans for rail or public transportation systems. The bill would require a designated rail or public transportation system to conduct a vulnerability assessment and to prepare and implement a security plan

that addresses the vulnerabilities identified in the assessment. Under the bill, a designated rail or public transportation system would include commuter, freight, and passenger rail systems, ferry systems, and intracity or intercity bus systems. Many of those transportation systems are private-sector entities. According to industry and government sources, a large number of those entities are currently engaged in activities similar to the assessment and planning that would be required under the bill. The incremental cost of complying with those requirements would depend on regulations that have not yet been issued, and therefore, CBO has no basis to estimate the cost to the private sector.

Security screening inspection claims

Section 914 would impose a new private-sector mandate on certain individuals filing claims for civil damages as a result of a security screening inspection. The bill would provide liability protection for transportation security officers or employees of the United States if the officer or employee performed such inspection in good faith. Because the bill would eliminate existing rights to seek compensation for damages caused by security inspectors, it would impose a private-sector mandate. The direct cost of the mandate would be the forgone net value of awards and settlements in such claims. According to DHS, there are no claims currently filed for such civil damages, and the amount of past settlements have been small relative to UMRA's annual threshold. Therefore, CBO expects that the number of future claims and the value of settlements and awards that would occur in the absence of this legislation would be small, if any.

Recurrent aircraft training

Section 916 would impose a new mandate on individuals applying for recurrent training to operate aircraft having maximum take-off weight of more than 12,500 pounds by requiring them to pay a fee for threat assessment as determined by DHS. The fee would be used to properly identify the individual and to determine if the individual is a present risk to aviation or national security. According to DHS, about 20,000 individuals would be required to pay this new fee, and the fee would most likely be $75 per individual. Therefore, CBO estimates that the direct cost of complying with the mandate would be about $1.5 million per year.

Prohibited items on passenger aircraft

Section 927 would impose a new mandate on airline crews and passengers by prohibiting scissors of any length (except ostomy scissors shorter than four inches) and certain tools such as screwdrivers, wrenches, and pliers from being carried aboard a passenger aircraft. Under current regulations, those items are allowed to be carried aboard passenger aircraft. According to government sources, the cost of complying with the mandate would be minimal, if any.

Department of Homeland Security name, initials, insignia, and seal

Section 1001 would impose a mandate prohibiting individuals and entities from using specific words, initials, titles, insignia, or the seal of DHS in connection with certain activities without writ-

ten permission. The bill would expand restrictions beyond those in current law. The cost of the mandate would be the cost of acquiring written permission from the department or the forgone net value attributable to such uses in the event that permission is not granted. Based on information from DHS, CBO expects that the direct cost to comply with the mandate would be minimal.

Previous CBO estimate: On March 29, 2006, CBO transmitted a cost estimate for S. 1052, the Transportation Security Improvement Act of 2005, as reported by the Senate Committee on Commerce, Science, and Transportation on February 27, 2006. S. 1052 would authorize the appropriation of specific amounts over the 2007–2009 period for security-related programs carried out by TSA within DHS, particularly for aviation security. Because H.R. 5814 would authorize additional appropriations in 2010, our estimate of total security-related spending under that bill is higher than under S. 1052.

Estimate prepared by: Federal Costs: DHS—Mark Grabowicz; Transportation Security—Megan Carroll. Impact on State, Local, and Tribal Governments: Sarah Puro and Melissa Merrell. Impact on the Private Sector: Paige Piper/Bach.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

COMPLIANCE WITH HOUSE RESOLUTION 1000

In compliance with H. Res. 1000, (109th Congress), the Committee verifies that no provision in this bill provides authority, including budget authority, or recommends the exercise of authority, including budget authority, for a contract, loan, loan guarantee, grant, loan authority, or other expenditure with or to a non-Federal entity.

ADVISORY COMMITTEE STATEMENT

This legislation creates the following advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act:

Section 403(a) amends the Homeland Security Act of 2002 to include a new section 1804, which requires the Secretary of Homeland Security, in consultation with the Secretary of Defense and the Secretary of State, to establish a Homeland Security Canine Detection Accreditation Board. This Board must be comprised of experts in the fields of canine training and explosives detection from Federal and State agencies, universities, other research institutions, and the private sector. The Board is responsible for developing and implementing national voluntary consensus standards for the accreditation of entities certifying canine detection teams.

Section 601(a) amends the Homeland Security Act of 2002 to include a new section 1912, which provides for the creation of an Advisory Council on Nuclear Detection to ensure that the work of each agency contributes to the deployment of an effective and efficient global nuclear and radiological detection architecture. The

Council must consist of five members appointed by the Director of the Domestic Nuclear Detection Office. Members must possess knowledge and technical expertise related to nuclear and radiological detection research and development and radiation detection. Members may not be employees of the Federal Government, other than employees of National Laboratories.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 1, which grants Congress the power to provide for the common Defense of the United States.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Title I—Authorization of Appropriations

Section 101. Department of Homeland Security

This section authorizes $34,698,270,000 for the necessary expenses of the Department of Homeland Security for Fiscal Year 2007.

Title II—Improving Management, Integration, and Oversight

Subtitle A—Management Reform

Section 201. Abolishment of the Under Secretary for Management

This section amends the Homeland Security Act of 2002 (P.L. 109–296) (6 U.S.C. 341) to eliminate the position of Under Secretary for Management. The Committee believes the current structure of the Department of Homeland Security (DHS or Department) does not provide sufficient authority to the Department's chief operating officers (Chief Financial Officer, Chief Information Officer, Chief Human Resources Officer, Chief Procurement Officer, Chief Administrative Officer, and Chief Security Officer) to efficiently and effectively provide their respective support services. Collectively, these officers are responsible for ensuring that the Department has appropriate and cost-effective management systems, policies, and procedures in place to support the operations of Departmental components and provide accurate and timely information to the Secretary. The Under Secretary for Management represents an unnecessary and redundant layer of bureaucracy that impedes rather than facilitates effective leadership. The abolishment of the Under Secretary for Management, as well as the enhancement of chief operating officers' authorities will improve communication and coordination through a direct reporting relationship to the Secretary, thereby elevating the standing of the chief

operating officers within the DHS organization and enabling them to more effectively fulfill their responsibilities.

Section 202. Providing direct line authority for chief operating officers

This section strengthens the ability of the Department of Homeland Security's (DHS) chief operating officers (Chief Financial Officer, Chief Information Officer, Chief Human Resources Officer, Chief Procurement Officer, Chief Administrative Officer, and Chief Security Officer) to ensure that their counterparts within the Department adhere to the laws, rules, regulations, and policies the chief operating officers are responsible for implementing.

Several reports issued by the Department's Office of Inspector General highlight weak management at the Department, including the inability to implement policies across the Department and secure the cooperation of personnel within the component agencies who are responsible for carrying out their respective support functions. The Committee believes that the Department's current structure provides insufficient support and authority to the chief operating officers, limiting their ability to oversee the implementation of policies, rules, and regulations regarding the budget, activities, planning, operations, and training of their counterparts in component agencies. Therefore, this section specifically vests each chief operating officer with the authority to direct the budget, activities, planning, operations, and training of their counterparts within the component agencies of the Department.

Section 203. Emergency planning and response for individuals with disabilities

This section amends the Homeland Security Act of 2002 (P.L. 107–296), to specify that the Officer for Civil Rights and Civil Liberties will serve as the Secretary's coordinator for emergency planning and response for individuals with disabilities. Acting as the Disability Coordinator, the Officer for Civil Rights and Civil Liberties is required to assist Departmental components in developing, implementing, and periodically reviewing policies and procedures regarding persons with disabilities.

This section would also establish a disability coordinator within both the Federal Emergency Management Agency (FEMA) and the Preparedness Directorate. The Committee believes this change will ensure the needs of individuals with disabilities are appropriately considered and incorporated in all emergency response plans.

Section 204. Government Accountability Office study on accessibility of emergency shelters

This section directs the Government Accountability Office to conduct a study of the accessibility of emergency shelters for individuals with disabilities. The Committee believes it is important to consider the needs of the physically disabled, as well as those who may have visual, hearing, or cognitive disabilities, in emergency response plans. In reviewing the effectiveness of emergency preparedness and response plans after the 2005 hurricane season, the Committee found that the needs of individuals with disabilities may not be adequately incorporated into Federal, State, local, and Tribal plans—particularly as they pertain to emergency shelters. For in-

stance, in addition to the need to construct special access ramps to allow wheelchair-bound individuals to access trailers and mobile homes, it was found that the doorways of many of these temporary homes were too narrow to permit the passage of a wheelchair. The Committee supports this review to determine if emergency shelters, as they currently exist, are adequate and accessible to persons with disabilities.

Section 205. Homeland Security Education Program

This section directs the Secretary of Homeland Security (Secretary), acting through the Assistant Secretary for Training and Exercises, to establish a graduate-level Homeland Security Education Program (Program) in the National Capital Region.

The Committee finds that important unmet requirements exist in the National Capital Region for graduate-level education to prepare government officials in senior homeland security, emergency management, and counterterrorism assignments at the Federal, State, Tribal, and local levels. The Committee further notes that the Department of Homeland Security (DHS or Department) has already funded the development of a Department-reviewed Master's Degree curriculum in homeland security, which currently is being implemented outside the National Capital Region.

This section, therefore, directs DHS to leverage this proven, Department-approved Master of Arts curriculum, and utilize the expertise of the institutions already delivering this curriculum to maximize efficiency and effectiveness in the Program's development and execution. Such leveraging will include the use of existing learning materials, quality assessment tools, digital libraries, exercise programs, and other curriculum components.

This section authorizes the Under Secretary of Emergency Management (Under Secretary) to designate students, who are officials from Federal, State, Tribal, and local governments, as well as from other sources designated by the Under Secretary. The Under Secretary shall also establish policies governing student enrollment and selection criteria, consistent with the Program's mission. In doing so, the Under Secretary shall take reasonable steps to ensure diversity among the student body.

The Committee intends that students in the Program will continue to serve in their public sector capacity for at least two years after receiving training through the Program. If an official who completes training separates from his or her agency position prior to the two-year period, that official would be required to reimburse the Government on a pro rata basis for the expenses incurred for the time remaining in the two-year period. Appropriate exemptions are included in this subsection.

The Committee requests the Under Secretary be responsible for specifying the Program's curriculum requirements. The Committee also expects the Under Secretary to establish appropriate policies governing the recruitment and governance of the Program's faculty, and for the identification of leadership positions within the Program necessary for its management. In establishing the Program's staffing and governance policies, the Under Secretary shall, to the maximum extent possible, leverage the faculty and collaborative governance arrangements already established between existing

DHS-sponsored Master's Degree graduate education and training programs.

Subtitle B—Integration and Organizational Improvements

Section 221. Establishment of Directorate for Policy, Planning, and International Affairs

This section amends the Homeland Security Act of 2002 (P.L. 107–296) to include a new "Title VI—Policy, Planning and International Affairs," which includes the following new sections.

Section 601. Directorate for Policy, Planning, and International Affairs

This section establishes a new Directorate for Policy, Planning, and International Affairs within the Department of Homeland Security, to be administered by an Under Secretary for Policy who will serve as the principal policy advisor to the Secretary, supervise and coordinate policy development, and ensure the budget of the Department is compatible with the Secretary's priorities.

Section 602. Office of International Affairs

This section transfers the Office of International Affairs, established in Section 879 of the Homeland Security Act of 2002 (P.L. 107–296), and elevates that Office's director to the rank of Assistant Secretary.

Section 603. Other offices and officials

This section also establishes the following offices and positions within the Directorate: an Office of Policy, to be administered by an Assistant Secretary for Policy; an Office of Strategic Plans, to be administered by an Assistant Secretary for Strategic Plans, and which will include a Secure Border Initiative Program Office and a Screening Coordination and Operations Office; an Office of the Private Sector; a Victim Assistance Officer; a Tribal Security Officer; and a Director of Cargo Security Policy.

The Victim Assistance Officer will coordinate and serve as the point of contact for individuals affected by a terrorist attack or natural disaster, and their families. The Victim Assistance Officer will coordinate with relevant officials throughout the Department to facilitate the dissemination of information regarding assistance programs and other forms of aid that may be available in the wake of a disaster, as well as to coordinate other concerns raised by affected individuals. The Victim Assistance Officer also will coordinate Departmental responses to victims with similarly situated officials at the Federal Bureau of Investigation, the National Transportation Safety Board, and other Federal agencies which respond to an act of terrorism or natural disaster.

The Tribal Security Officer will serve as the single point of contact for tribal governments across the United States and its territories. Currently, Indian tribes, as defined by section 4(e) of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b(3)), many of which are located along the Nation's borders and in border states, have unique concerns to address with the Department, and have difficulty sharing and receiving important information from the Department. The Tribal Security Officer shall coordi-

nate the flow of information and ensure that tribal concerns are appropriately considered in the development and implementation of Departmental policies and programs.

The Director of Cargo Security Policy will operate under the direction and control of the Under Secretary for Policy. The responsibilities of the Director will include: advising the Assistant Secretary for Policy regarding all Departmental cargo security programs, policies, and initiatives; developing Department-wide cargo security policies; and coordinating Departmental cargo security policies and programs with other Federal departments and agencies. The Director's coordination role includes working with officials of the Department of Energy and the Department of State in recognition of international cargo security agreements.

Section 222. Consolidation of the Efforts of the Center for Domestic Preparedness and the Noble Training Center

This section transfers the Noble Training Center to the Center for Domestic Preparedness (CDP). All programs offered by the Noble Training Center will be incorporated into the CDP's program structure. Both the Noble Training Center and the CDP are located at Fort McClellan, a former Army base, in Anniston, Alabama. The Committee believes that this transfer will strengthen the effectiveness and efficiency of the training programs offered by both facilities.

To support the expansion of the CDP, this section designates the CDP Director as a member of the executive service. The Committee believes that the increase in designation will ensure the Director has the administrative authority to match the expanding responsibilities of the CDP.

This section also authorizes the Director of the CDP to obtain the transfer of the Army In-Processing Center and the Noncommissioned Officer Housing Dormitories. Both of these facilities are located at Fort McClellan and are currently leased by the CDP from the Joint Powers Authority, which administers the facilities. The CDP's planned expansion will require additional training space to adequately accommodate program participants. The Committee urges the CDP to work with the necessary authorities to quickly complete this facility transfer.

Section 223. Government Accountability Office study of integration and adequacy of training programs related to asylum at ports of entry

This section requires the Government Accountability Office (GAO) to conduct a review of the training provided to border security personnel who interdict, interview, and process asylum seekers at ports of entry, including airports. The study shall include: an assessment of whether such training provides such personnel with adequate and clear guidance on the standards for handling asylum seekers; an assessment of whether such personnel coordinate appropriately to ensure that relevant United States laws are fully enforced; and, recommendations for steps that the Secretary of Homeland Security should take to provide better integration and adequacy of such training to such personnel in order to better secure the borders of the United States while ensuring that asylum seekers are properly processed and their claims are fully evaluated.

Subtitle C—Strengthening Oversight

Section 231. Congressional notification requirement

This section directs the Secretary of Homeland Security to inform both the House Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs of current Departmental activities. This section is similar to Congressional notification requirements in place for other Cabinet Departments.

The Committee believes that communication between the Department and Congressional Committees needs to be enhanced. The requirement under this section for the Department to notify Congress of its activities is intended to improve the flow of information and thereby enhance oversight and monitoring of the Department.

Section 232. Authorization Liaison Officer

This section directs the Chief Financial Officer of the Department of Homeland Security to establish an Authorization Liaison Officer within the Department. The Authorization Liaison Officer will provide timely budget and other financial information to the House Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs. This section also requires the Authorization Liaison Officer to coordinate with the Office of the Chief Financial Officer to ensure that all budget and financial reports prepared for the Congress are submitted concurrently to the appropriate Committees.

In order to be thoroughly informed on the performance of the Department, the authorizing Committees of jurisdiction must receive budget and financial reports which are currently provided to the House and Senate Appropriations Committees. The Authorization Liaison Officer within the Department will facilitate the sharing of this information.

Section 233. Required line item for Office of Counternarcotics Enforcement

This section requires a line item in the budget for the Office of Counternarcotics Enforcement to strengthen the Office's authority over its general budget. The Committee believes that designating a line item in the Federal budget for the Office of Counternarcotics will raise the profile of this important component of the Department of Homeland Security and strengthen the Office's ability to perform its mission to stop the entry of illegal drugs into the United States.

Section 234. Secure Border Initiative financial accountability

This section directs the Inspector General of the Department of Homeland Security to review each contract action related to the Department's Secure Border Initiative (SBI) having a value of $20,000,000 or more. This review will determine whether each action fully complies with applicable cost requirements; performance objectives; program milestones; requirements for the inclusion of small, minority, and women-owned businesses; and applicable timelines. The Inspector General's review must occur not later than 60 days after the date of the initiation of the action and upon the conclusion of the performance of the contract. The Inspector Gen-

eral is required to submit a report to the Secretary of Homeland Security containing the findings of the review, including findings regarding any cost overruns, significant delays in contract execution, lack of rigorous departmental contract management, insufficient departmental financial oversight, bundling that limits the ability of small businesses to compete, or other high risk business practices.

This section further directs the Secretary, not later than 30 days after the receipt of each required report, to submit to the appropriate congressional committees (as defined in section 102(g) of the Homeland Security Act of 2002 (P.L. 107–296)) a report on the findings of the Inspector General and the steps the Secretary has taken, or plans to take, to address the problems identified in the report.

To further ensure the cost-effectiveness of SBI, the Committee urges the Secretary to carefully consider utilizing low-cost persistent surveillance capabilities and existing, proven technologies for land, sea, and aerial surveillance, including unmanned aerial vehicles (UAVs), remote piloted airship vehicles, gyroplanes, and other aerial platforms. The Committee believes it is important to closely monitor the development and implementation of the new SBI. The Committee is concerned about the extent of mismanagement of SBI's predecessor border surveillance program, the Integrated Surveillance and Intelligence System (ISIS), particularly the numerous operational problems and financial irregularities in the Remote Video Surveillance component of ISIS. This section is intended to ensure the mistakes of the past are not repeated in the implementation of the more expensive and more complex SBI.

Title III—Procurement Reform

Section 301. Homeland Security procurement training

This section requires the Chief Procurement Officer (CPO) of the Department of Homeland Security (DHS) to provide procurement training to acquisition employees. It requires the CPO to coordinate Departmental acquisition education programs and tailor them to support the career development of acquisition employees, develop the curriculum for homeland security procurement training, establish training standards and requirements for acquisition employees, and develop a system to maintain student enrollment records.

This section also establishes a Council on Procurement Training to advise the CPO regarding policy and curriculum recommendations. The Deputy Chief Procurement Officer would serve as the Chairman of the Council, which would be composed of the chief procurement officers of the Department's eight procurement offices.

This section reflects concerns raised by the Inspector General in reports and testimony presented before the Subcommittee on Management, Integration, and Oversight regarding the lack of qualified procurement officers within the Department. This section addresses the concerns of the Inspector General and is intended to strengthen the skills of the procurement officers within DHS.

Section 302. Additional requirements to review past performance contractors

This section strengthens the review process prior to the awarding of a contract by requiring contract bidders to submit information regarding the contractor's past and current performance on contracts for Federal, State, local, and Tribal governments, and the private sector. Under this section, contracting officers of the Department are required to review the performance information provided and contact the relevant official who oversaw any contract performed by the contractor in question during the five-year period preceding the contract award.

The Committee has reviewed the Department's contracting process and found instances where specific business owners who were awarded Department contracts had criminal records and/or poor performance on previous contracts. The Committee believes that mandating a review of a contractor's past and current performance will help limit fraud, waste, and abuse.

Section 303. Streamlining of SAFETY Act and procurement processes

This section requires the Secretary of Homeland Security to ensure that a sufficient number of personnel trained to apply economic, legal and risk analyses are involved in the review and prioritization of anti-terrorism technologies for the purpose of determining whether those technologies may be designated or certified by the Secretary under the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act), (6 U.S.C. 441, Title VIII, Subtitle G of (P.L. 107–296)). The Secretary is also required to ensure coordination for implementing the SAFETY Act among the Chief Procurement Officer, the Under Secretary for Science and Technology, the Under Secretary for Policy, and the General Counsel, and ensure coordination of the Department's efforts to promote awareness and utilization of the SAFETY Act at the Federal, State, and local level.

The section requires the Department to issue a directive to implement the SAFETY Act regulations, and provide SAFETY Act training for all acquisition employees. In addition, the Secretary is required to conduct a review of all ongoing and anticipated procurement, and provide a report to Congress identifying those that may be appropriate for the application of the risk and litigation management benefits of the SAFETY Act, and identifying the steps the Department is taking to ensure those benefits are being fully utilized.

Section 304. Comptroller General report on Department of Homeland Security contracting

This section requires the Government Accountability Office (GAO) to examine the contracting procedures of the Department of Homeland Security, and submit a report to the Congress not later than six months after the date of enactment. This report would include the findings of the Comptroller General with respect to any improvements in such procedures that could be made through the use of new technologies.

Through a series of hearings the Committee became ware of discrepancies in the contracting practices of the Department were un-

covered. The Committee believes that a review by the Comptroller General will determine the extent to which poor contracting practices exist within the Department, and may support implementation of an established standard to ensure all contracts within the Department are administered effectively.

Section 305. Contracting requirements

This section requires the Secretary of Homeland Security to require any offeror for any Department of Homeland Security contract to submit as part of the offeror's bid an attestation that affirmatively discloses any substantial role the offeror or the offeror's company or employees may have played in creating the solicitation, request for proposal, statement of work, or statement of objectives for the Department. This section also requires the Secretary to require any offeror who submits an attestation disclosing that the offeror played a substantial role in creating a solicitation, request for proposal, statement of work, or statement of objectives for the Department, to submit a description of the safeguards in place to prevent the offeror from receiving information through such a role that could have provided the offeror with an undue advantage in submitting an offer for a contract.

The intent of this section is to respond to an issue that came to light in a series of hearings held by the Committee where it was discovered that, in certain cases, DHS was using contractors to develop solicitations and requests for proposals, for which those same contractors (or related companies) would submit bids and be awarded contracts. The Committee intends this section to enhance the contracting process within the Department by providing more transparency and preventing current contractors from gaining undue advantages on future contract awards through their involvement with the development of solicitations.

Section 306. Certification requirements for offerors for Department of Homeland Security contracts

This section requires any contractor submitting an offer for a Department of Homeland Security (DHS) contract to submit a written certification that the business is not in default or arrears on its payment of Federal taxes. The Government Accountability Office has found that 60,000 Federal contractors owe a total of $6 billion in Federal taxes. The Committee believes that payment or non-payment of Federal taxes is important information regarding a contractor's financial history and should be considered by DHS procurement officers prior to a contract award.

Section 307. Contracts for assistance activities relating to acts of terrorism, natural disasters, and other emergencies

This section amends the Homeland Security Act of 2002 (P.L. 107–296) to require the Secretary of Homeland Security (or the head of any Departmental component) to work towards a goal of awarding not less than 20 percent of the total value of contracts awarded for debris removal, supply distribution, reconstruction, or other activities related to an act of terrorism, natural disaster, or other emergency, to qualified firms located in the affected area. This section also encourages the award of such contracts to small and disadvantaged businesses, and encourages such contracts to be

negotiated prior to an act of terrorism, natural disaster, or other emergency.

Through the Committee's investigation into the contracting practices of the Department after Hurricane Katrina, the Committee found that greater involvement by local businesses in debris removal and reconstruction activities could assist in more efficient recovery from future disasters. In addition, Federal, State, local, and Tribal governments could save taxpayers' dollars and improve the speed of response and recovery by negotiating prices for necessary goods and services well in advance of a disaster, at which time more full and open competition is possible.

Section 308. Emergency Contracting Support Annex

This section directs the Secretary of Homeland Security to update the National Response Plan to establish a Support Annex on "Emergency Contracting." Specifically, the Support Annex should set forth plans and protocols for incident-related contracting to meet urgent needs in the event of acts of terrorism, natural disasters, and other emergencies. Given the widespread contracting problems in the aftermath of Hurricanes Katrina and Rita, the Committee believes that such an annex will help the Federal government implement a more effective and efficient process for bidding and negotiating contracts to provide necessary goods and services, such as ice, food, water, debris removal, and temporary housing.

Section 309. Increased Inspector General oversight

This section authorizes $108,685,000 for the Office of the Inspector General for Fiscal Year 2007. The Committee recognizes the increasing oversight responsibilities of the Office of the Inspector General. This authorization will enable the Office of the Inspector General to meet increasing demands to review, audit, and investigate the rapidly increasing number of Departmental programs, contracts, and grants.

Section 310. Purchase cards

This section requires the Department of Homeland Security (DHS) to review and strengthen its policies regarding the use of purchase cards, and ensure that each Departmental employee issued a purchase card is informed of its proper use. A review by the Government Accountability Office found that poor training, lax oversight, and general confusion about how the Department-issued purchase cards should be used have resulted in inappropriate purchases by DHS employees. Therefore, this section is intended to strengthen the Department's management of purchase cards and reduce the opportunities for waste, fraud, and abuse.

Title IV—Personnel Authorities

Subtitle A—Workforce Enhancements

Section 401. Cost-effective training for Border Patrol agents

This section contains provisions intended to reduce the overall costs of hiring, training, and deploying new Border Patrol agents. This section waives certain course requirements for trainees and requires a competitive sourcing study to be conducted to compare

the costs of training new Border Patrol agents at non-profit or private training facilities.

This section also places a $150,000 cap on the costs to hire, train, and deploy a new Border Patrol agent. If costs exceed the $150,000 cap, the Secretary of Homeland Security must certify the costs to the Committee on Homeland Security in order to continue training.

The Committee conducted a thorough examination of the costs associated with training Border Patrol agents, and found that Customs and Border Protection (CBP) was not able to provide sufficient detail or otherwise justify the costs of training. By placing a cap on training costs, the Committee hopes to increase accountability and encourage CBP to improve the efficiency of hiring, training, and deploying new agents.

Section 402. Continuation of Federal Law Enforcement Training Center authority to appoint and maintain a cadre of Federal annuitants to support training.

This section expands current authority held by the Federal Law Enforcement Training Center (FLETC) to hire Federal retirees for training purposes. This authority permits Department of Homeland Security agencies that conduct training at FLETC to utilize the expertise of retired personnel to teach new recruits, rather than pulling active personnel away from their assigned duties. This section extends this authority for five years from the date of enactment and increases the number of annuitants that may be hired from 250 to 350.

Section 403. Canine Detection Team coordination and certification

This section directs the Secretary of Homeland Security to coordinate the Department's canine training programs; maximize the use of existing training facilities and resources to train canines throughout the year; and coordinate the use of detection canines trained by other Federal agencies, non-profit organizations, universities, and private training facilities in order to increase the number of trained detection canines available to Federal, State, and local law enforcement agencies.

In addition, this section encourages domestic breeding of canines suitable for detection training, establishes a Homeland Security Canine Detection Accreditation Board within the Department of Homeland Security (DHS) to certify the canine detection training and testing processes and procedures used by other entities, and forbids the use of homeland security grant funds to purchase a detection canine team that has not been certified under the voluntary process established by the accreditation board.

Through its investigations, the Committee has found that canines are an effective tool against terrorism and are used effectively to support the homeland security and other protective missions of a number of Federal agencies. Canine detection teams are used by Federal, State, local, and Tribal government agencies and the private sector to detect explosives, narcotics, people, and other concealed matter. The Committee believes that greater numbers of canine detection teams are needed to support homeland security missions. A panel of experts from Federal and local law enforcement agencies, research institutions, and the private sector, indicated in testimony before the Committee that the need exists for

a National canine detection team certification and accreditation process to protect the public from the safety and security risks posed by ineffective or insufficient canine detection team training.

Section 404. Authority for Customs and Border Protection to appoint and maintain a cadre of Federal annuitants

This section provides United States Customs and Border Protection (CBP) with temporary authority to rehire up to 500 annuitants to provide necessary surge capacity until the Border Patrol has a sufficient number of trained Border Patrol agents to maintain operational control of the Nation's borders. Currently, the Border Patrol has a force of approximately 12,000 agents. It is estimated that a force of 18,000 to 20,000 agents will be necessary, along with the implementation of border technologies, to secure the Nation's borders.

While the Border Patrol is aggressively working to hire and train new agents, the authority provided by this section will permit CBP to utilize the wealth of experience and expertise held by annuitants to train and supervise new Border Patrol agents, as well as to meet the demand for highly trained agents to patrol the Nation's land borders. This authority is a short-term solution intended to help meet an immediate security need. The Committee recognizes the value of this action, but specifically instructs the Department to take note that using such employees ultimately may have a negative impact on the Department's budget over the long-term. While rehired annuitants receive less in salary and benefits than their non-annuitant counterparts, they continue to receive retirement distributions in addition to their new salary.

Nothing in this provision is intended to limit rights to which employees are otherwise entitled under the law.

Section 405. Strengthening Border Patrol recruitment and retention

This section directs the Secretary of Homeland Security to establish a plan to increase the recruitment and retention of Border Patrol agents. Such plans should focus on providing incentives to Border Patrol agents, including the payment of bonuses, increases in the pay percentage differentials for agents living in high-cost areas, and mechanisms to allow agents to transfer locations after the first two years of service.

The intent of this section is to help United States Customs and Border Protection (CBP) recruit and retain a top quality border patrol workforce. The Committee has investigated the issue of recruitment and retention bonuses and believes that if CBP were able to offer additional recruitment and retention incentives to agents, experienced agents would be less willing to relocate to another agency, department, or branch of service. In addition, by allowing CBP to offer additional recruitment incentives, highly skilled individuals would be attracted to the force.

Section 406. Customs and Border Protection Officer pay equity

This section grants law enforcement officer status to any individual serving as a Customs and Border Protection Officer for the purposes of Federal pay and retirement benefits. Such benefits are available retroactively from the creation of the Department of Homeland Security on March 1, 2003.

The Committee appreciates the dedicated law enforcement work of legacy employees from the Departments of Justice and Treasury who currently serve in the Department of Homeland Security. These individuals currently serve as Customs and Border Protection Officers under DHS's One Face at the Border Initiative to streamline the inspection process at ports of entry. It should be noted that, while United States Customs and Border Protection (CBP) was created in March 2003, the title "Customs and Border Protection Officer" was not adopted until July 2004. Therefore, for the purposes of this section, the definition of "prior qualified service" applies to predecessor positions held by CBP enforcement personnel including Customs inspectors, Canine Enforcement Officers, and Immigration Inspectors as of March 2003.

Based on its oversight, the Committee recognizes that many duties of these officers formerly included law enforcement activities such as the investigation or apprehension of individuals suspected or convicted of criminal offenses, and many of these officers were authorized and trained to carry firearms.

The Committee also recognizes that the law enforcement responsibilities of these individuals may have been expanded upon their joining the Department of Homeland Security. The Committee, therefore, encourages the Secretary, in coordination with the Director of the Office of Personnel Management, to review the previous work and training of these individuals in their former capacities with respect to the recognition of their prior law enforcement duties. The changes implemented by this section recognize the hard work of these men and women who help secure our Nation's borders.

Subtitle B—Improving Security Clearance Process

Section 411. Increased security screening of homeland security officials

This section requires the Secretary of Homeland Security to conduct a Department-wide examination of the security clearance and suitability review procedures for Department employees and contractors, as well as individuals in State and local government agencies and private sector entities with a need to receive classified information. The Secretary is directed to take appropriate steps, based on the findings of this review, to strengthen the Department's security policies, including consolidating the security clearance investigative authority at the Department's headquarters.

The Committee has reviewed serious examples of criminal conduct by departmental officials, including a contract awarded to a company whose owner had multiple felony convictions and a poor business record. As a result of such findings, the Committee determined that security screening practices within the Department should be strengthened. This section requires a Department-wide review to ensure the Department's security screening practices are improved.

Section 412. Authorities of Chief Security Officer

This section amends the Homeland Security Act of 2002 (P.L. 107–296) to establish a Chief Security Officer in the Department of Homeland Security who will have responsibility for personnel se-

curity, security awareness, and security training. The Chief Security Officer must also ensure that all Departmental components comply with Federal standards for security clearances and background investigations.

Title V—Intelligence and Information Sharing

Section 501. Departmental reorganization

Following the completion of the Department of Homeland Security's (DHS) Second Stage Review, in July of 2005, the Secretary of Homeland Security re-named the Office of Information Analysis and gave it responsibilities in addition to those outlined under the Homeland Security Act of 2002 (P.L. 107–296). In addition to its statutory duties, one of the major responsibilities for the new Office of Intelligence and Analysis is to serve as the Chief Intelligence Office of DHS, thereby taking responsibility for leading the Intelligence Components of the Department.

While the Committee agrees with the consolidation of the duties of the Office of Intelligence and Analysis, the Committee also believes that the powers of the DHS Chief Intelligence Officer (CINT) can only be effectively wielded by an Undersecretary. Therefore, this section amends Homeland Security Act of 2002 to restructure the Department to reflect the changes the Secretary made following the Second Stage Review, and elevates the Assistant Secretary for Information Analysis to Under Secretary for Intelligence and Analysis (I&A).

The section also assigns additional responsibilities to I&A to institute a clearer relationship between the CINT and the DHS Intelligence Components. Successful implementation of this section should result in a strengthened Departmental intelligence capability, allowing information and intelligence from the borders, ports, critical infrastructure, and state and local government to be seamlessly fused into an intelligence product that is truly national. While the Department has taken many solid steps in this direction since the completion of the Second Stage Review in July 2005, the Committee believes that the Secretary must redouble efforts to better integrate DHS intelligence components internally.

Section 502. Intelligence components of Department of Homeland Security

This section assigns responsibilities for the Department of Homeland Security's (DHS) Intelligence Components to coordinate and support the Directorate of Intelligence and Analysis (I&A). It also directs the Secretary to establish training for Intelligence Components to ensure consistency in the information being shared with I&A and to develop a Department-wide intelligence culture and to facilitate the exchange of information among and between DHS intelligence partners.

This section defines "Intelligence Components" as "any directorate, agency, or element of the Department that gathers, receives, analyzes, produces, or disseminates homeland security information." It specifically excludes the units required to be maintained as distinct entities, namely the Coast Guard and Secret Service. Internal DHS document and physical security responsibilities are

also excluded because these efforts are part of the Department's management and internal security responsibilities.

Section 503. Homeland Security Advisory System

The color-coded Homeland Security Advisory System has been used several times in its relatively brief history, but has, for the most part, been accompanied by little to no information of interest to the homeland security community. While the system has improved over time, this section ensures that the Homeland Security Advisory System will include information on appropriate protective measures and countermeasures and is limited, when appropriate, to specific regions, localities, or sectors.

Section 504. Homeland Security Information Sharing

This section directs the Department of Homeland Security (DHS) to establish a Department-wide Information Sharing Environment (ISE). The Committee believes it is essential that the DHS intelligence operation be fully integrated and have full connectivity with the broader Federal ISE. It is vitally important that the Secretary of Homeland Security continue to support the President's efforts to better integrate the National Intelligence Community through the work of the Program Manager of the Department's ISE.

This section also directs the Secretary to designate "Information Sharing and Knowledge Management Officers" at each Intelligence Component to coordinate information sharing efforts and direct the development of feedback mechanisms to State, Local, Tribal, and private sector entities. To date, the Committee has found that the Department's outreach to State, local, and Tribal intelligence and law enforcement officials has been haphazard, and often accompanied by less than immediate results. While there have been many successful examples of coordination and collaboration with non-Federal officials, the Office of Intelligence and Analysis must increase its involvement with State and local officials and incorporate this non-Federal information into DHS intelligence products. It is essential that DHS provide feedback to non-Federal contributors to both encourage their contributions and provide helpful guidance for future contributions.

Section 505. State, Local, Tribal, and Regional Information Fusion Center initiative

This section directs the Secretary of Homeland Security to establish an initiative to coordinate the Department of Homeland Security (DHS) intelligence efforts with State, Local, Tribal, and Regional Fusion Centers; assist Fusion Centers with carrying out their homeland security duties; and facilitate information sharing efforts between Fusion Centers and the Department. State, local and regional fusion centers are being successfully established across the country due to the initiative of State and local law enforcement and intelligence services. The Committee believes that the DHS Office of Intelligence and Analysis, which has primary responsibility for sharing information with State, local, and Tribal officials, needs to play a stronger, more constructive role in assisting these centers, and notes that the Department has taken steps to do so.

The Committee strongly believes that the State, local, Tribal and Regional Fusion Center Initiative is a key to Federal information-sharing efforts and must succeed in order for the Department to remain relevant in the blossoming State and local intelligence community. As part of the Committee's oversight responsibilities, the Committee has visited many of the State and city Fusion Centers successfully established across the Nation. The Committee applauds these State and local efforts and the dedication of those who staff these centers. The Department has a responsibility to support these centers, and the Committee is pleased to see that the Department has begun doing so. However, DHS must act quickly, thoroughly, and cooperatively in order to provide the maximum amount of support for these State and local centers.

Section 506. Homeland Security Information Sharing Fellows Program

This section directs the Under Secretary for Information and Analysis within the Department of Homeland Security (DHS) to establish a fellowship program for State, local, and Tribal officials to rotate into Intelligence and Analysis (I&A) in order to facilitate State, local, and Tribal understanding of the sharing process, assist DHS I&A's understanding of their information needs, and to assist in dissemination of homeland security information.

This section will compliment the fusion center initiative, giving State, local, and Tribal officials better insight and input into the Department's information sharing operations and allowing them to play a greater role in the DHS information sharing effort.

Section 507. Full and efficient use of open source intelligence

This section directs the Under Secretary for Information and Analysis within the Department of Homeland Security (DHS) to fully utilize open source information. While the Committee understands the Department has been improving its open source acquisition and analysis capabilities, the Committee nonetheless encourages DHS to work closely with the Assistant Deputy Director of National Intelligence (ADDNI) to maximize federal open source intelligence efforts.

Additionally, this section directs the Under Secretary for Information and Analysis to perform analysis of critical infrastructure information that is available in the public domain. Al-Qa'ida has shown a determination to use open source information, including Government Accountability Office (GAO) reports and public information on critical infrastructures. DHS must look at that same information from the perspective of terrorists in order to recognize vulnerabilities.

Section 508. Strengthening the capabilities of the Human Smuggling and Trafficking Center

This section provides necessary funding and resources to enhance the capabilities of the Human Smuggling and Trafficking Center (HSTC) by transferring the responsibility for providing administrative support and funding for staffing, operating, and maintaining the HSTC to the Assistant Secretary of U.S. Immigration and Customs Enforcement. This section further requires the HSTC to coordinate and share homeland security information with the Office

of Intelligence and Analysis, and directs the Secretary of Homeland Security to execute a Memorandum of Understanding with the Attorney General of the United States to clarify responsibility for handling human smuggling, human trafficking, and terrorist travel cases.

While the Committee values the unique role of each agency participating in the HSTC and the ongoing commitment of resources to this effort, the Committee believes U.S. Immigration and Customs Enforcement has the appropriate experience and historical perspective on human smuggling and trafficking issues to assume responsibility for operating the HSTC and leading its interagency efforts. In operating the HSTC, the Assistant Secretary for U.S. Immigration and Customs Enforcement is authorized to seek reimbursement from the U.S. Departments of Justice and State for the costs associated with operating the HSTC.

Title VI—Preventing Nuclear and Biological Terrorism

Section 601. Establishment of Office of Domestic Nuclear Detection

This section formally authorizes the creation and activities of the Domestic Nuclear Detection Office (DNDO). The DNDO was first established by joint Presidential Directive HSPD–14/NSPD–43 (National Security Presidential Directive NSPD–43/Homeland Security Presidential Directive HSPD–14) on April 15, 2005. Under the leadership of an appointed Director, the DNDO is responsible for: developing a global nuclear detection architecture, implementing the domestic portion of the architecture, performing transformation research and development to improve detection capabilities, and maintaining situational awareness of the nuclear and radiological threat.

This section grants the Director of the DNDO the same hiring authorities as the Homeland Security Advanced Research Projects Agency, which are designed to attract highly qualified technical personnel, and establishes an Advisory Council on Nuclear Detection and an Interagency Coordination Council to ensure that the work of each agency contributes to the deployment of an effective and efficient global detection architecture.

This section also requires technology development and acquisition programs within DNDO to make use of a rigorous testing program to provide a "bottom line" assessment of capabilities prior to deployment. The Committee acknowledges that, in the past, technologies have been acquired and deployed without full knowledge of their true capabilities. This section will ensure that performance capabilities under realistic operating conditions will be known. For newly developed, advanced detection systems, this section will enable verification that desired capabilities have been attained. The Committee believes this requirement is vital to ensure that effective detection technologies are deployed to counter the nuclear and radiological threat, and that the Federal government is making good use of nuclear detection funding.

Section 602. Chief Medical Officer

This section formally authorizes the creation of the Office of the Chief Medical Officer (CMO) as a primary focal point within the Department of Homeland Security (DHS) for handling medical

issues related to acts of terrorism, natural disasters, or other emergencies. The Secretary of Homeland Security established the CMO in July 2005, following the "Second Stage Review" of the Department's structure and operations. Prior to the establishment of the CMO, the Department had no centralized medical structure for coordinating medical preparedness activities within DHS or with other Departments across the Federal government.

The Committee believes that formally establishing the CMO will ensure that DHS is able to effectively oversee medical preparedness and response activities and coordinate with other Federal agencies on these matters. The CMO will play a critical role in preparing for a possible influenza pandemic or other emerging diseases that threaten National security, and provide guidelines for medical response plans to State and local first responders. The Committee believes that DHS needs dedicated staff to coordinate and integrate medical preparedness and response activities into overarching emergency response plans. The CMO will provide the critical on-site expertise necessary to ensure effective DHS leadership on medical and public health emergency preparedness and response.

Section 603. National Biosurveillance Integration System

This section formally authorizes the National Biosurveillance Integration System (NBIS) to ensure the continued development of this surveillance component as part of an integrated strategy for biodefense. The NBIS, which is overseen by the Chief Medical Officer (CMO), is a comprehensive system designed to integrate and fuse relevant surveillance data from public and private sources to rapidly recognize and characterize the dispersal of biological agents in human and animal populations, food, water, agriculture, and the environment.

The Committee believes that NBIS will enhance the Nation's capability to provide early warning of a biological event, whether terrorist-related or naturally occurring, and provide continuous biosituational awareness. This system is being built upon and reinforces existing Federal, State, local, international, and private sector surveillance systems, and incorporates relevant threat analysis information from the Intelligence Community. DHS, in cooperation with other appropriate Federal departments and agencies, integrates these efforts and disseminates assessments to appropriate Federal, regional, State, and local response entities to support decision-making.

To accomplish the NBIS mission, the CMO is charged with seeking appropriate data feeds; facilitating the two way flow of information from State and local governments; ensuring the integration of intelligence information; and hiring personnel, or requesting detailees from its interagency partners, with the needed expertise. Because NBIS requires near real-time surveillance data from multiple agencies to be an effective detection system, the Committee encourages DHS to focus resources on meeting the challenge of obtaining interagency cooperation.

This section also creates the interagency Joint Biosurveillance Leadership Council to provide guidance and recommendations for NBIS to the CMO. The Committee believes that this surveillance system will provide the earliest warnings of a biological attack and

thus enable Federal, State, and local entities to appropriately respond as soon as possible.

Section 604. Material threats

This section modifies the Project BioShield Act of 2004 (P.L. 108–276), to accelerate and prioritize the Department of Homeland Security's (DHS) performance of Material Threat Assessments (MTAs) and Material Threat Determinations (MTDs). The Department of Health and Human Services (HHS) procures countermeasures under Project Bioshield, but before this procurement can take place, the Department must perform MTDs to identify whether a particular threat is credible and immediate, and conduct MTAs to provide information about the threat—such as an estimated number of exposed individuals, the geographical extent of the exposure, and other collateral effects.

The Committee is frustrated at the pace with which DHS is conducting and issuing MTAs and MTDs, and with the failure of DHS to notify Congress of MTDs as required by law. Currently, MTAs can take four to eight months to complete and the Committee knows of no process for prioritizing which MTAs to conduct. Because the acquisition process hinges on completion of MTAs and MTDs, procurement under Project BioShield has been slow. The Committee believes this section is necessary to accelerate the rate at which MTAs and MTDs are completed so that the Federal government can more quickly procure the chemical, biological, radiological, and nuclear (CBRN) medical countermeasures required for National defense.

Section 605. Biosafety laboratory training needs

Over the next five years, the Federal Government will invest in over 2.6 million gross square feet of new construction involving Bio-Safety Level (BSL) 3 and BSL 4 laboratory space in order to support the development of countermeasures against the threat of bioterrorism. Early estimates show that full deployment of these facilities could require over 3,000 trained personnel. This section requires the Secretary of Homeland Security to work with the Secretary of Defense and the Secretary of Health and Human Services to examine the current status of staffing at BSL 4 facilities and to determine the number of newly trained staff that will be needed as these new Federally-supported facilities are completed and become operational. The study should determine specific training requirements, including the needs for curriculum development, to fully staff existing and planned BSL 4 facilities so as to ensure their safe and efficient operation. The Committee encourages the Department to partner with a university that is experienced in operating a BSL 4 facility in order to determine the staffing needs, training requirements, and opportunities for a coordinated national biocontainment training program.

Section 606. Homeland Security Science and Technology Advisory Committee

This section authorizes the extension of the Homeland Security Science and Technology Advisory Committee (HSSTAC) to ten years from the date it was established. Congress established the HSSTAC to provide independent, scientific, and technical planning

advice to the Under Secretary for Science and Technology. When the charter for the HSSTAC expired in 2005 the organization was immediately dissolved by DHS officials. The Committee believes that the independent advisory services of the HSSTAC and its scientific expertise is crucial to the success of DHS's Science and Technology mission.

Title VII—Homeland Security Infrastructure Protection and Cybersecurity Enhancement

Section 701. Infrastructure protection and cybersecurity

This section amends Title II of the Homeland Security Act of 2002 (P.L. 107–296) by adding a new "Subtitle E—Infrastructure Protection and Cybersecurity," which consists of the following sections 241 and 242.

Subtitle E—Infrastructure Protection and Cybersecurity

Section 241. Office of Infrastructure Protection

This section authorizes the creation of an Office of Infrastructure Protection headed by an Assistant Secretary for Infrastructure Protection (Assistant Secretary). This legislative change is necessary because the Office of Infrastructure Protection was originally authorized as part of the Information Analysis and Infrastructure Directorate under Title II of the Homeland Security Act of 2002 (P.L. 107–296). The Office of Infrastructure Protection and the Information Analysis Division have since been separated under the Secretary of Homeland Security's reorganization authority, and this section merely codifies the existing structure.

Under this section, the Assistant Secretary has the primary authority for all Department critical infrastructure protection programs, including policy formation and program management. One of the major responsibilities of the Assistant Secretary will be to identify and carry out comprehensive risk assessments of critical infrastructure to determine the risks posed by particular types of terrorist attacks.

This section also requires the Assistant Secretary to develop and maintain a comprehensive National plan for securing the key resources and critical infrastructure of the United States. The Committee recognizes the need for closer coordination, and, therefore, requires the Assistant Secretary to work with other Federal, State, local, and Tribal government agencies when conducting vulnerability assessments and recommending infrastructure protection measures. While the vulnerability assessments are focused specifically on acts of terrorism, the Committee recognizes that in developing the National Infrastructure Protection Plan, the Office of Infrastructure Protection must take into consideration all-hazards, including the adoption of protective measures to prevent acts of terrorism.

This section further requires the Assistant Secretary to establish and maintain partnerships and information sharing processes with Federal, State, local, and Tribal governments, the private sector, and international governments and organizations. The Assistant Secretary must work with the Under Secretary for Intelligence and Analysis and elements of the intelligence community to coordinate

information with Federal, State, local, and Tribal law enforcement agencies, and the private sector.

It is critically important for the Department to take an all-hazards approach to infrastructure protection. As such, this section mandates that the Assistant Secretary assess preparedness capabilities of critical infrastructure to mitigate against, respond to, and recover from, acts of terrorism and other catastrophic emergencies.

In order to ensure the Secretary is well versed on all activities of the Office of Infrastructure Protection, the Assistant Secretary is required to provide the Secretary with an annual summary of National critical infrastructure protection efforts and priorities. In addition, the Assistant Secretary is responsible for providing the Secretary, in consultation with the Assistant Secretary for Grants and Planning, with recommendations for Federal critical infrastructure protection funding.

The Committee recognizes that although the Office of the Infrastructure Protection and the Office of Intelligence and Analysis are now organizationally separate, they must continue to coordinate and communicate to provide accurate and timely risk assessments. To achieve this goal, this section requires the creation of an integration center to be staffed from the Office of Infrastructure Protection, the Office of Cybersecurity and Telecommunications, and the Office of Intelligence and Analysis. This integration center better reflects the current organization of the Department and the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). The responsibilities of this center is to integrate threat, vulnerability, and consequential information to identify priorities for protective measures, and disseminate analytical products.

Sec. 242. Office of Cybersecurity and Telecommunications

This section establishes an Office of Cybersecurity and Telecommunications administered by an Assistant Secretary. This Assistant Secretary is responsible for all Department cybersecurity-related critical infrastructure programs, including policy formation and program management. The Assistant Secretary's specific duties include establishing and managing a national cybersecurity response system, a national cybersecurity threat and vulnerability reduction program, and a national cybersecurity awareness and training program. Given the rapid convergence of data and telephony, this section also provides the Assistant Secretary with primary authority to create and administer an emergency communications program.

The Committee encourages the Assistant Secretary for Cybersecurity and Telecommunications to request that State Homeland Security Directors develop a State cybersecurity strategy with a focus on continuity of operations and disaster recovery strategies for the critical information and communications technology systems and technology assets that support emergency services at the State and local levels. The Assistant Secretary should encourage States to conduct risk and need assessments that take into account the multitude of threats to relevant cyber systems. The Assistant Secretary should also encourage coordination with State Homeland Security Directors and State Chief Information Officers, to jointly develop a State cybersecurity strategy for critical information and communications technology systems.

Another area of importance to the Committee is the promotion and distribution of cybersecurity best practices. The responsibilities of the Assistant Secretary include promoting voluntary cybersecurity best practices and benchmarks that are responsive to rapid technology changes and to the security needs of critical infrastructure. As such, the Committee encourages DHS to consider the roles of Federal, State, local, and foreign governments; appropriate standards bodies; and the private sector, including the insurance industry and auditors, to develop methods to promote the wider use of cybersecurity across the economy. The Committee recognizes that, due to the interconnectedness of information networks, a weakness in one sector may have a cascading effect across other sectors. With this in mind, the Department is expected to work with the private sector and academia to determine the best mechanisms for developing a distribution system for cybersecurity best practices and benchmarks to all end user groups across economic sectors, as well as students and government entities.

Section 702. Critical infrastructure study

This section directs the Secretary of Homeland Security, in consultation with other appropriate Federal agencies and National organizations representing architecture, engineering, surveying, and mapping professional organizations, to conduct a study to determine whether architecture, engineering, surveying, or mapping activities related to critical infrastructure are being sent offshore and what, if any, vulnerabilities or threats exist, and to recommend necessary steps to protect National and homeland security interests.

Section 703. Cybersecurity training program and equipment

There is a growing need for well trained experts in the field of cybersecurity to ensure that information systems are as secure and reliable as possible, both now and in the future. This section authorizes the Assistant Secretary for Cybersecurity and Telecommunications to establish, in conjunction with the National Science Foundation, a program to award grants to institutions of higher education in order to establish or expand cybersecurity profession development and associate degree programs. These grants may also be used to purchase equipment to provide cybersecurity training for either the professional or associate degree programs.

This section defines the roles of the Assistant Secretary and the Director of the National Science Foundation. Specifically, the Assistant Secretary shall establish the goals of the program and determine the criteria for awarding the grants. The Director shall operate the program and consult with the Assistant Secretary in selecting awardees. This section authorizes the transfer of $3,700,000 from the Department to the National Science Foundation in Fiscal Year 2007, for the funding of these grants.

Section 704. National asset database

This section provides the Secretary of Homeland Security direction on the use and management of the National Asset Database (NADB), a national asset inventory. The NADB serves as a primary data repository that may be used for the analysis and integration required to provide the Department of Homeland Security

(DHS) with the capability to identify, catalog, and maintain a list of critical national assets. This section requires an annual report to the Committee on Homeland Security on the status of the NADB; the "at most risk" critical infrastructure list; any changes in defining and identifying critical infrastructure; and the extent to which the database is used as a tool for allocating funds to prevent, reduce, mitigate, and respond to terrorist attacks. DHS is required to meet annually with the States to provide guidance, gain clarification, and seek verification. It also requires DHS to remove assets that are determined to be unverifiable and to not meet national asset guidelines.

Title VIII—Grants Administration

Section 801. Faster and smarter funding for first responders

Subsection (a) amends the Homeland Security Act of 2002 (P.L. 107–296) by adding at its end a new "Title XX—Funding for First Responders," which consists of the following sections 2001–2005.

Section 2001. Definitions

This section provides a number of definitions, such as the terms "covered grant," "first responder," and "terrorism preparedness."

Section 2002. Faster and smarter funding for first responders

Subsection (a) states that the provisions of the new Title XX apply only to those grants that the Department of Homeland Security (DHS) provides to States, regions, or directly eligible Tribes for the primary purpose of improving the ability of first responders to prevent, prepare for, respond to, mitigate against, or recover from threatened or actual terrorist attacks—especially those involving weapons of mass destruction. Specifically, such terrorism preparedness grants are those administered under the State Homeland Security Grant Program, the Law Enforcement Terrorism Prevention Program, and the Urban Area Security Initiative.

Subsection (b) expressly excludes from coverage of this title all non-DHS Federal grants, as well as the DHS firefighter assistance grants and the emergency management planning and assistance grants.

Section 2003. Covered grant eligibility and criteria

This section provides that States, regions, and directly eligible Tribes may apply for covered grants. To be eligible to receive a covered grant, however, a State must first submit to the Secretary of Homeland Security a comprehensive three-year State homeland security plan tied to the achievement, maintenance, and enhancement of the essential capabilities established. Such a plan must be developed in consultation with, and subject to, appropriate comment by local governments, Tribes, and first responders within the State. This section also sets forth the minimum application requirements to receive grants. The Secretary may not approve any State, regional, or Tribal application that is inconsistent with any State plan.

Section 2004. Risk-based evaluation and prioritization

This section establishes a First Responder Grant Board (Grant Board)—composed of a broad cross-section of officials from the Department of Homeland Security—to assist the Secretary in awarding covered grants to States, regions, and directly eligible Tribal governments. Specifically, the Grant Board shall evaluate and prioritize all covered grant applications on the basis of risk. In doing so, the Grant Board must consider a number of factors including, but not limited to: the threat to, vulnerability of, and consequences for persons (including transient commuting and tourist populations) and critical infrastructure; prior acts of international terrorism; elevations in the threat alert level; the most current risk assessment of the threats of terrorism against the United States; and other types of threats. Prior to evaluating and prioritizing all pending applications for covered grants, however, the Grant Board shall provide an opportunity for applicants to provide information to the Grant Board regarding the "risk profile" of the applicants' jurisdictions.

After evaluating and prioritizing all covered grant applications on the basis of risk, the Grant Board shall then ensure that each State, territory, and up to twenty directly eligible Tribes receive no less than a defined minimum amount of funding. The minimum threshold for each of the States, the District of Columbia, and Puerto Rico is 0.25 percent of the total funds available for covered grants that fiscal year. Because of the unique terrorism preparedness needs of States with international borders, this section provides a minimum threshold of 0.45 percent of the total funds available for covered grants that fiscal year for each State that has a significant international land border or adjoins a body of water within North America through which an international boundary line extends. The minimum threshold for the U.S. Virgin Islands, the Territories of American Samoa and Guam, and the Commonwealth of the Northern Mariana Islands is 0.08 percent of the total funds available for covered grants that fiscal year. The minimum threshold for directly eligible Tribes, collectively, is 0.08 percent of the total funds available for covered grants that fiscal year.

In awarding covered grants to regions, the Committee urges the Grant Board to ensure, to the maximum extent practicable, that such funds are distributed among the jurisdictions that could reasonably be expected to provide support to the region in the event of a terrorist attack. Moreover, the Committee believes that such distributions should be made on the basis of the risk profile of subareas within each region.

Section 2005. Use of funds

This section provides a list of permitted and prohibited uses of covered grant funds. Specifically, a covered grant may be used for appropriate activities as determined by the Secretary of DHS, including: personnel costs directly attributable to elevations in the threat alert level issued by a State, region, or local government; personnel expenses for individuals dedicated exclusively to counterterrorism and intelligence activities; and training and exercises to assist public elementary and secondary schools in developing terrorism preparedness programs.

A covered grant, however, may not be used to supplant State or local funds; construct buildings or other physical facilities, such as barriers, fences, and gates, except those constructed under the terms and conditions of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 USC § 5121 et seq.) and the cost of which do not exceed the greater of $1,000,000 per project or, if approved by the Secretary, up to ten percent of the total amount of the covered grant; to acquire land; or alleviate any State or local government cost sharing contribution.

Subsection (b) of section 801 amends the definition of "emergency response provider" in the Homeland Security Act of 2002 (P.L. 107–296) to clarify that the fire service and Governmental and non-Governmental organizations and personnel are included in the definition.

Section 802. Authorization of appropriations

This section authorizes that, of the amount authorized under section 101, $2,900,000,000 be appropriated for Fiscal Year 2007 for covered grants.

Section 803. Metropolitan medical response system

This section authorizes the currently existing, but unauthorized, Metropolitan Medical Response System (MMRS). It directs the Assistant Secretary for Grants and Planning to administer grants to develop, maintain, and enhance medical preparedness and response systems to ensure they are capable of responding effectively during the initial hours of a public health crisis or mass-casualty event. Grant recipients may use funds to enhance their medical preparedness and response capabilities, such as, medical surge capacity; mass prophylaxis; chemical, biological, radiological, nuclear, and explosive detection, response, and decontamination capabilities; triage and pre-hospital treatment; medical supply management and distribution; and fatality management. This section authorizes $60 million in funds for each of the Fiscal Years 2007 through 2010, an amount double the funding for recent fiscal years.

The increased funding for the MMRS program will enable jurisdictions to achieve an enhanced capability to respond to weapons of mass destruction mass casualty events during the first hours so crucial to lifesaving and population protection, and before significant external assistance can arrive. In light of the risks posed by a possible pandemic influenza such as Influenza A virus subtype (H5N1) and other bio-hazards, the Committee believes it is imperative that the system is properly funded and maintains adequate resources.

Title IX—Transportation Security

Subtitle A—Rail and Public Transportation Security

Section 901. Transportation security

This section amends title IV of the Homeland Security Act of 2002 (P.L. 107–296) to include a new "Subtitle G—Transportation Security," which consists of the following sections.

Section 481. Rail and public transportation vulnerability assessments and security plans

This section requires the Secretary of Homeland Security to promulgate regulations that require a designated rail or public transportation system to conduct a vulnerability assessment and prepare and implement a security plan to address identified vulnerabilities. For the purposes of this section, a "designated rail or public transportation system" is defined to encompass rail, ferry, and bus transportation systems, including Amtrak. This section also provides specific requirements for vulnerability assessments and security plans.

This section allows the Transportation Security Administration (TSA) to recognize existing procedures, protocols, and standards in compliance with the requirement for vulnerability assessments and security plans. This section also allows co-located facilities to jointly develop plans and assessments. This section is enforced through civil penalties.

It is the intent of the Committee to ensure that the major public and rail transportation agencies in the United States have completed vulnerability assessments and have prepared and implemented facility security plans. It is the Committee's understanding that many agencies may have already completed such assessments and plans, and the Secretary should recognize these existing efforts.

Section 482. National rail and public transportation security plan

This section requires the Secretary of Homeland Security to update the National Strategy for Transportation Security (TSA) with a supplement on rail and public transportation security. This section requires that the plan leverage and take into consideration existing plans including the National Infrastructure Protection Plan and the Transportation Sector-Specific Plan.

The Transportation Security Administration (TSA) prepared and submitted a National Strategy for Transportation Security in 2005. The Committee, however, is disappointed with the lack of specificity in the plan. This section outlines the specific measures that need to be addressed in the Strategy. The Committee recognizes that TSA is in the process of developing (with the private sector and other Federal agencies) a transportation sector-specific plan for the National Infrastructure Protection Plan, due at the end of 2006. To the extent that the sector-specific plan meets the requirements, the Committee expects TSA to leverage such plan.

Section 483. Rail and public transportation strategic information sharing plan

This section requires the Secretary of Homeland Security to develop a plan to share tactical and strategic intelligence products relating to threats and vulnerabilities of the rail and public transportation system. This section also requires updates and annual reports on the intelligence distributed.

The Committee intends the Transportation Security Administration to prepare a plan to improve intelligence and information sharing with rail and public transportation agencies. This plan must be submitted to the Congress within ninety days.

Section 902. Rulemaking requirements

This section requires that the Secretary of Homeland Security issue an interim final rule to implement section 481 of the Homeland Security Act of 2002 (P.L. 107–296), as amended by Section 901. This section waives the provisions of the Administrative Procedures Act (5 U.S.C. 500) and stipulates that the final regulations must be issued within two years of enactment.

Section 903. Rail and public transportation security training program

This section requires the Department of Homeland Security to establish rail and public transportation security training guidance. The guidance developed should include a program that addresses: determination of the seriousness of an occurrence; crew and passenger communication; suspicious behavior recognition; evacuation procedures; and training exercises. This section requires that the program be consistent with national initiatives and conform to national voluntary consensus standards to be developed and promulgated by the Secretary.

Section 904. Interagency cooperation

This section requires the Secretary of Homeland Security to consider whether, in fulfilling the requirements of this title, a memorandum of agreement should be updated or executed with other Federal agencies, including the Department of Transportation (DOT).

The Committee recognizes that a general Memorandum of Agreement (MOA) was executed between DOT and the Transportation Security Administration in 2004. Recently, an annex to this agreement was signed regarding pipeline security and hazardous materials. The Committee believes that an additional annex regarding rail and public transportation security may be appropriate.

Section 905. Rail and public transportation security grant program

This section amends the Homeland Security Act of 2002 (P.L. 107–296) to establish a rail and public transportation security grant program to allocate funds based on risk. Grant awards will be prioritized based on the most current risk assessment and national economic and strategic defense considerations. This section requires the Secretary to issue guidelines for the establishment of accounting and reporting requirements to ensure that the grant money is used for the purposes for which they were provided.

Section 906. Rail and public transportation security exercise program

This section establishes a rail and public transportation security exercise program for the purpose of testing and evaluating the capabilities of Federal, State, and local agencies and appropriate rail and public transportation stakeholders to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism, natural disasters, and other emergencies.

The Committee believes that exercises based on real world scenarios can greatly improve the ability of transportation employees and first responders to respond to a terrorist attack. The response to recent attacks on other countries' public transportation systems

has shown that the response by first responders, front-line employees, and passengers can greatly decrease the loss of life during an attack. The exercise program in this section, along with the training program under section 903, will greatly improve the ability of rail and mass transit agencies to respond in the event of a terrorist attack.

Section 907. Authorization of appropriations

The section authorizes $400 million from the amounts authorized in section 101 for rail and mass transit security grants for Fiscal Year 2007.

It is the sense of the Committee that the current allocation of $150 million per fiscal year does not adequately address the needs of the Nation's rail and mass transit agencies in preparing for, and protecting against, acts of terrorism. The increase of $250 million will provide more grant funding to the agencies that need it most, as it will be allocated based on risk, in accordance with section 905 of this bill.

Subtitle B—Transportation Security Operations Enhancements

Section 911. Aviation security funding

This section amends 49 U.S.C. 48301 to extend the authorization of funding for aviation security activities through Fiscal Year 2010. The section also deletes an obsolete provision which authorized grants for Fiscal Year 2002 to air carriers for cockpit doors, video monitors, continuous use of transponders, and innovative technologies.

Section 912. Research and development of transportation security technology

This section amends section 137 of the Aviation Transportation Security Act (P.L. 107–71) (ATSA) to reauthorize research and development funding and grant authority through 2010 and expand coverage to all modes of transportation.

The Committee believes that the research and development authorized under ATSA should be extended through 2010 and move beyond aviation security to all modes of transportation. Research and development of technology is vital to securing a system as open and diverse as our mass transit and rail systems. The Committee acknowledges that leveraging technology, through modification of existing technology or through the development of new technology, can better secure all modes of transportation.

Section 913. Enforcement authority in non-aviation transportation

This section amends 49 U.S.C. 114, and 46301 to clarify the legal authority of the Secretary of Homeland Security to initiate administrative enforcement proceedings for violations of transportation security regulations and requirements relating to modes of transportation other than aviation.

The Committee is concerned that the Transportation Security Administration (TSA) does not currently have the authority to enforce security directives or regulations against non-aviation modes of transportation. This section ensures that the TSA has the authority to enforce regulations issued to all modes of transportation.

Section 914. Liability for security screening inspections

This section provides immunity from liability for civil damages to any officer or employee of the United States conducting an inspection pursuant to 49 U.S.C. 44901 or 44903 as long as the inspection is performed in good faith. This section also establishes the claims process under the Small Claims Act (31 U.S.C. §3723, P.L. 97–258), and authorizes the Transportation Security Administration to settle such claims administratively.

Section 915. Temporary private screener assistance

This section amends 49 U.S.C. 44920 to authorize the Secretary of Homeland Security (Secretary) to supplement the Federal airport security workforce with qualified private screeners during times of emergency, such as natural disasters, terrorist acts, or threats to national security, that create a surge in demand for screener capacity. This section authorizes the Secretary to establish conditions for temporarily contracting with private screener companies at airports operating under Federal screeners.

Section 916. Recurrent training to operate certain aircraft

This section authorizes the Secretary of Homeland Security to assess a fee to conduct a threat assessment of an individual engaged in recurrent flight training on an aircraft weighing more than 12,500 pounds. The section requires the Secretary, upon a determination that an individual is a risk to aviation or National security, to notify the flight school to prohibit training the individual, or terminate any training already in progress. The section exempts foreign military pilots endorsed by the Department of Defense from the fees prescribed by this section.

The Committee is concerned that students engaged in recurrent flight training are exempt from the statutory waiting period required for first time students, which enables a threat assessment to be completed. As changes will have been made to terrorist watchlists since prior training, the provision gives the Department authority to prudently perform a limited name-based threat assessment and to recover costs for those assessments.

Section 917. Annual report on unclaimed money recovered

This section requires the Secretary of Homeland Security to ensure that the Department maintains an accounting of the unclaimed monies recovered at airport security checkpoints, which are retained by the Transportation Security Administration pursuant to 49 U.S.C. 44945.

Subtitle C—Passenger Screening

Section 921. Passenger identification documents

This section amends the Homeland Security Act of 2002 (P.L. 107–296) to require the Transportation Security Administration (TSA) to develop standards and minimum requirements for determining airline passenger identification for passenger entry to a sterile area in any United States airport. In addition, this section requires that the TSA set training standards for document inspectors for recognizing unacceptable or fraudulent identifications. It also creates civil and criminal penalties for any individual who

knowingly presents a false identification document. The section further provides that passengers attempting to enter a sterile area without presenting an acceptable form of identification must undergo additional security screening as deemed appropriate by the TSA.

Section 922. International passenger prescreening

This section requires the Secretary of Homeland Security to conduct a pilot program to evaluate the use of automated systems for the immediate prescreening of passengers on flights in foreign transportation. The section also requires the Secretary to provide a report on the findings of the pilot program to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate. The Secretary is prohibited from issuing a final rule implementing the Advanced Passenger Information System (APIS) until the pilot program and subsequent report are completed.

Section 923. International cooperative efforts

This section encourages the Secretary of Homeland Security to pursue cooperative efforts toward establishing international technology standards for passenger data and collection systems.

Section 924. Computer Assisted Passenger Prescreening System

This section requires the Transportation Security Administration (TSA) to conduct a study of the Computer Assisted Passenger Prescreening System (CAPPS). The study must include the impact of CAPPS on passengers, the cost of administering CAPPS, and an evaluation of whether CAPPS screening should be continued after the deployment of the Secure Flight Program. The TSA must submit a report to the Committee on Homeland Security in the House of Representatives and, in the Senate, the Committee on Homeland Security and Government Affairs, and the Committee on Commerce, Science, and Transportation. This section also requires the TSA to develop a system to ensure that passengers who have completed fingerprint based background checks or hold DOD clearances are exempt from secondary screening under CAPPS.

Section 925. Federal flight deck officers

This section amends 49 U.S.C. 44921 to: provide Federal flight deck officers (FFDOs) with an option for their training dates, improve FFDO travel access to training facilities, establish qualification standards for facilities that offer requalification and recurrent training, and eliminate the cost for training for eligible pilots. The section also prescribes standards for the revocation of FFDO status. In addition, this section directs the Secretary of Homeland Security to implement a pilot program to enable FFDOs to retain and carry weapons. This section also encourages the President to pursue agreements with foreign governments to allow the maximum deployment of FFDOs on international flights and provide a report to Congress on the status of such efforts.

Section 926. Enhanced security and access control through comprehensive screening of airport workers

This section requires the Transportation Security Administration (TSA) to conduct a pilot program at five commercial service air-

ports to physically screen all airport workers with access to secure and sterile areas of the airport. The section establishes certain parameters for the pilot program, including the manner of screening and the type of airports involved, and requires that a report be issued to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate within 90 days of the completion of the pilot program. The report must include an assessment of the impact, benefits, and costs of screening all workers.

Section 927. Prohibited items

The section directs the Transportation Security Administration (TSA) to prohibit tools and scissors of any length, with the exception of ostomy scissors shorter than four inches, from being carried aboard a passenger aircraft.

Section 928. Secured areas of airports

This section requires the Transportation Security Administration (TSA) to issue regulations and take other appropriate measures to implement the requirements of 49 U.S.C. 44903(h)(3) pertaining to access to secured areas of airports. The section further requires the establishment of a schedule for airports to update their security plans following TSA's fulfillment of this section.

Section 929. Foreign repair stations

This section directs the Transportation Security Administration (TSA) to issue regulations or enact other appropriate measures for the implementation of the requirements of 49 U.S.C. 44924 pertaining to foreign repair stations. Should the TSA fail to take the necessary actions, the section compels TSA to issue a weekly report that sets forth the reasons for missing the deadline and provides an update of its progress towards complying with this section.

Subtitle D—Technical Amendments

Section 931. Reporting requirements repealed

Subsection (a) repeals sections 607 and 608 of Vision 100—Century of Aviation Authorization Act (P.L. 108–176) requiring that the Under Secretary for Border and Transportation Security provide a certification on eight specific efficacy criteria for the Transportation Security Administration's (TSA) Computer Assisted Passenger Screening Program (CAPPS II).

Subsection (b) repeals Section 109(b) of Aviation Transportation Security Act (ATSA) (P.L. 107–71), which requires an annual report on the progress the Administrator of the TSA has made in evaluating and determining whether to take various specific actions to enhance transportation security.

Subsection (c) repeals 49 U.S.C. 44942 requiring an annual report on the establishment of measurable goals and objectives "consistent with the requirements of the Government Performance and Results Act of 1993 (GPRA) . . ." The information required is independently provided as part of the reporting process under the GPRA.

This section eliminates duplicative oversight reports while ensuring that the Congress will continue to receive information that it

requires for oversight purposes. It is the Committee's intent to, wherever possible, reduce the number of reports required by the TSA and the Department of Homeland Security, while ensuring that the Congress receives the necessary information to conduct oversight.

Section 932. Consolidation of reports

This section amends 49 U.S.C. 44938 to consolidate, into a single report, the requirements for an annual report on transportation security, and a biennial report on screening and foreign air carrier and airport security.

Section 933. Aircraft charter customer and lessee prescreening

This section makes technical corrections to section 4012 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (P.L. 108–408). By inserting the word "certificated," it applies section 4012's requirements for aircraft charter customer and lessee prescreening to aircraft "with a maximum certificated takeoff weight of 12,500 pounds or more." Thus, this section aligns the requirements of section 4012 of the IRTPA with the authority conferred on the Transportation Security Administration by section 132(a) of the Aviation Transportation Security Act (P.L. 107–71).

Title X—Miscellaneous Provisions

Section 1001. Protection of Department of Homeland Security Official Seal and Insignia

This section provides the Department of Homeland Security with copyright protections over its seal, name, initials, and the titles of its officers. This protection is similar to statutory protections for visual representations of seals of other Federal agencies. This section specifically requires written permission from the Secretary to use the name, initials, seal, or titles of the Department in connection with any advertisement, commercial activity, movie, television show, or other audiovisual production, impersonation, internet domain name, e-mail address, web site, merchandise, or solicitation in a manner intended to convey the impression that the Department has approved, endorsed, or authorized such use.

Names, initials, seals, or titles protected by this section include: the words "Department of Homeland Security;" the initials "DHS;" the insignia or seal of the Department; the title "Secretary of Homeland Security;" the name, initials, insignia, or seal of any organizational element (including any former such element) of the Department; or the title of any other officer or employee of the Department. This section empowers the Attorney General of the United States to initiate civil proceedings to enjoin unauthorized potential uses of representations of the Department.

The Committee intends this section to provide the Department the ability to control the use of its name, initials, seal, titles, and other representations in order to enhance public awareness about its mission and programs, and prevent misrepresentations or false impressions. Without this statutory protection, the Department may encounter difficulty preventing misuse and taking corrective action when it occurs.

Section 1002. Authorized use of surplus military vehicles

This section requires the Secretary of Homeland Security to include United States military surplus vehicles that have demonstrated utility for responding to acts of terrorism, emergencies, and other disasters on the Standardized Equipment List, in order to allow States and localities to purchase, modify, upgrade, and maintain such vehicles using homeland security assistance administered by the Department. This section specifically includes the M–113 and other qualifying military surplus vehicles on the Standardized Equipment List for use by States and local jurisdictions for homeland security purposes.

Section 1003. Encouraging use of computerized training aids

This section authorizes the Secretary of Homeland Security to use and make available to State and local agencies computerized training aids—such as the Advanced Conflict and Tactical Simulation, a Government-owned computer modeling program, in order to improve the abilities of municipalities to prepare for, and respond to, a chemical, biological, or other terrorist attack.

Section 1004. Emergency notification system study deadline

This section sets a deadline for the Secretary of Homeland Security to submit a final report on the nationwide emergency notification system study required in section 7403 of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108–408). Although the Department was required to submit a report by August 2005, an initial report was submitted to the Congress in March 2006, and no final report has been received. The Committee is disappointed by the lengthy delay in complying with the requirements of section 7403 and strongly urges the Secretary to complete the study and issue a final report.

Section 1005. Report on fraud prevention exercises

This section requires that, within 180 days of enactment, the Secretary of Homeland Security submit a report to the Congress on the feasibility of devising an exercise program to test and evaluate the capabilities of Federal, State, local, and Tribal governments to detect and prevent fraud, waste, and abuse in Federal assistance programs administered in response to acts of terrorism, natural disasters, and other emergencies.

Section 1006. Limitation on reimbursements relating to certain detailees

This section prohibits an individual detailed to the Department of Homeland Security from receiving compensation for services that exceed the maximum rate of pay allowable to a member of the Senior Executive Service. The Committee has found that certain individuals detailed to the Department are paid well above the maximum salary allowable on the Senior Executive Service pay scale. The use of detailees may provide Departmental components with needed expertise. These assignments, however, are intended to be temporary and should not create wide imbalances among Departmental employees or conflicts of interest due to extraordinarily high compensation rates.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.

* * * * * * *

TITLE I—DEPARTMENT OF HOMELAND SECURITY

* * * * * * *

Sec. 104. Congressional notification.

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

Subtitle A—Directorate for Information Analysis and Infrastructure Protection; Access to Information

[Sec. 201. Directorate for Information Analysis and Infrastructure Protection.]
Sec. 201. Office of Intelligence and Analysis.

* * * * * * *

Sec. 203. Intelligence components.
Sec. 204. Homeland Security Advisory System.
Sec. 205. Homeland security information sharing.
Sec. 206. Comprehensive information technology network architecture.
Sec. 207. State, Local, Tribal, and Regional Information Fusion Center Initiative.
Sec. 208. Homeland Security Information Sharing Fellows Program.
Sec. 209. Full and efficient use of open-source intelligence.

* * * * * * *

Subtitle E—Infrastructure Protection and Cybersecurity

Sec. 241. Office of Infrastructure Protection.
Sec. 242. Office of Cybersecurity and Telecommunications.

* * * * * * *

TITLE IV—DIRECTORATE OF BORDER AND TRANSPORTATION SECURITY

* * * * * * *

Subtitle G—Transportation Security

Sec. 481. Rail and public transportation vulnerability assessments and security plans.
Sec. 482. National rail and public transportation security plan.
Sec. 483. Rail and public transportation strategic information sharing plan.
Sec. 484. Passenger identification documents.

TITLE V—EMERGENCY PREPAREDNESS AND RESPONSE

Sec. 501. Under Secretary for Emergency Preparedness and Response.

* * * * * * *

Sec. 510. Procurement of security countermeasures for strategic national stockpile.
Sec. 511. Urban and other high risk area communications capabilities.
Sec. 512. Contracts for assistance activities relating to acts of terrorism, natural disasters, and other emergencies.

Sec. 513. Chief Medical Officer.
Sec. 514. Rail and public transportation security grant program.

[TITLE VI—TREATMENT OF CHARITABLE TRUSTS FOR MEMBERS OF THE ARMED FORCES OF THE UNITED STATES AND OTHER GOVERNMENTAL ORGANIZATIONS

[Sec. 601. Treatment of charitable trusts for members of the Armed Forces of the United States and other governmental organizations.]

TITLE VI—POLICY, PLANNING, AND INTERNATIONAL AFFAIRS

Sec. 601. Directorate for Policy, Planning, and International Affairs.
Sec. 602. Office of International Affairs.
Sec. 603. Other offices and officials.
Sec. 604. Consultation on trade and customs revenue functions.

TITLE VII—MANAGEMENT

[Sec. 701. Under Secretary for Management.]
Sec. 701. Deputy Secretary.

* * * * * * *

Sec. 707. Chief Security Officer.

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

Subtitle A—Coordination with Non-Federal Entities

Sec. 801. Office for State and Local Government Coordination.
Sec. 802. Rail and public transportation security training program.
Sec. 803. Rail and public transportation security exercise program.

* * * * * * *

Subtitle H—Miscellaneous Provisions

Sec. 871. Advisory committees.

* * * * * * *

[Sec. 879. Office of International Affairs.]

* * * * * * *

Sec. 890A. Homeland security procurement training.

* * * * * * *

TITLE XVIII—MISCELLANEOUS PROVISIONS

Subtitle A—Canine Detection Teams

Sec. 1801. Coordination and enhancement of canine detection team training.
Sec. 1802. Canine procurement.
Sec. 1803. Domestic canine breeding grant program.
Sec. 1804. Homeland Security Canine Detection Accreditation Board.
Sec. 1805. Definitions.

Subtitle B—Treatment of Certain Charitable Trusts

Sec. 1811. Treatment of charitable trusts for members of the armed forces of the United States and other governmental organizations.

TITLE XIX—DOMESTIC NUCLEAR DETECTION

Sec. 1901. Office of Domestic Nuclear Detection.
Sec. 1902. Responsibilities of Director of Domestic Nuclear Detection.
Sec. 1903. Global nuclear detection architecture.
Sec. 1904. Research and development.
Sec. 1905. System assessments.
Sec. 1906. Technology acquisition, deployment, support, and training.
Sec. 1907. Situational awareness.
Sec. 1908. Forensic analysis.
Sec. 1909. Threat information.
Sec. 1910. Administrative authorities.
Sec. 1911. Report requirement.
Sec. 1912. Advisory Council on Nuclear Detection.

Sec. 1913. Interagency coordination council.
Sec. 1914. Authorization of appropriations.
Sec. 1915. Definitions.

TITLE XX—FUNDING FOR FIRST RESPONDERS

Sec. 2001. Definitions.
Sec. 2002. Faster and Smarter Funding for First Responders.
Sec. 2003. Covered grant eligibility and criteria.
Sec. 2004. Risk-based evaluation and prioritization.
Sec. 2005. Use of funds.

SEC. 2. DEFINITIONS.

In this Act, the following definitions apply:

(1) * * *

* * * * * * *

(6) The term "emergency response providers" [includes Federal, State, and local emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.] *includes Federal, State, and local governmental and nongovernmental emergency public safety, law enforcement, fire, emergency response, emergency medical (including hospital emergency facilities), and related personnel, organizations, agencies, and authorities.*

* * * * * * *

(17) The term "intelligence component of the Department" means any directorate, agency, or element of the Department that gathers, receives, analyzes, produces, or disseminates homeland security information except—

(A) a directorate, agency, or element of the Department that is required to be maintained as a distinct entity under this Act; or

(B) any personnel security, physical security, document security, or communications security program within any directorate, agency, or element of the Department.

* * * * * * *

TITLE I—DEPARTMENT OF HOMELAND SECURITY

* * * * * * *

SEC. 103. OTHER OFFICERS.

(a) DEPUTY SECRETARY; UNDER SECRETARIES.—There are the following officers, appointed by the President, by and with the advice and consent of the Senate:

(1) * * *

(2) An Under Secretary for [Information Analysis and Infrastructure Protection] *Intelligence and Analysis*.

* * * * * * *

[(7) An Under Secretary for Management.]

[(8)] *(7)* A Director of the Office of Counternarcotics Enforcement.

[(9)] *(8)* Not more than 12 Assistant Secretaries.

[(10)] *(9)* A General Counsel, who shall be the chief legal officer of the Department.

* * * * * * *

(d) OTHER OFFICERS.—To assist the Secretary in the performance of the Secretary's functions, there are the following officers, appointed by the President:

(1) * * *

* * * * * * *

(5) A Director of the Domestic Nuclear Detection Office.

* * * * * * *

SEC. 104. CONGRESSIONAL NOTIFICATION.

(a) IN GENERAL.—The Secretary shall actively consult with the congressional homeland security committees, and shall keep such committees fully and currently informed with respect to all activities and responsibilities within the jurisdictions of these committees.

(b) RELATIONSHIP TO OTHER LAW.—Nothing in this section affects the requirements of section 872. The requirements of this section supplement, and do not replace, the requirements of that section.

(c) INSPECTOR GENERAL.—The Inspector General of the Department shall be responsible, independently of the responsibility of the Secretary under subsection (a), for keeping the congressional homeland security committees fully and currently informed of the Department's activities, including informing the congressional homeland security committees of major audits, investigations, or other activities of the Inspector General by no later than 72 hours prior to the release of, or at any time upon the request by such a committee for, the findings of major audits, investigations, or other activities. Additionally, the Inspector General shall provide to such a committee a written notification and summary of the contents of its semiannual and annual reports by no later than 72 hours prior to the release of such reports.

(d) CLASSIFIED NOTIFICATION.—The Secretary may submit any information required by this section in classified form if the information is classified pursuant to applicable national security standards.

(e) SAVINGS CLAUSE.—This section shall not be construed to limit or otherwise affect the congressional notification requirements of title V of the National Security Act of 1947 (50 U.S.C. 413 et seq.), insofar as they apply to the Department.

(f) DEFINITION.—As used in this section, the term "congressional homeland security committees" means the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate.

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

Subtitle A—Directorate for Information Analysis and Infrastructure Protection; Access to Information

[SEC. 201. DIRECTORATE FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION.

[(a) UNDER SECRETARY OF HOMELAND SECURITY FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION.—]

SEC. 201. OFFICE OF INTELLIGENCE AND ANALYSIS.

(a) UNDER SECRETARY OF HOMELAND SECURITY FOR INTELLIGENCE AND ANALYSIS.—

(1) IN GENERAL.—There shall be in the Department [a Directorate for Information Analysis and Infrastructure Protection] *an Office of Intelligence and Analysis* headed by [an Under Secretary for Information Analysis and Infrastructure Protection] *an Under Secretary for Intelligence and Analysis*, who shall be appointed by the President, by and with the advice and consent of the Senate.

* * * * * * *

[(b) ASSISTANT SECRETARY FOR INFORMATION ANALYSIS; ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION.—

[(1) ASSISTANT SECRETARY FOR INFORMATION ANALYSIS.—There shall be in the Department an Assistant Secretary for Information Analysis, who shall be appointed by the President.

[(2) ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION.—There shall be in the Department an Assistant Secretary for Infrastructure Protection, who shall be appointed by the President.

[(3) RESPONSIBILITIES.—The Assistant Secretary for Information Analysis and the Assistant Secretary for Infrastructure Protection shall assist the Under Secretary for Information Analysis and Infrastructure Protection in discharging the responsibilities of the Under Secretary under this section.]

[(c) DISCHARGE OF INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION.—] *(b) DISCHARGE OF INTELLIGENCE AND ANALYSIS.—* The Secretary shall ensure that the responsibilities of the Department regarding information analysis [and infrastructure protection] *and intelligence* are carried out through [the Under Secretary for Information Analysis and Infrastructure Protection] *the Under Secretary for Intelligence and Analysis*.

[(d)] *(c)* RESPONSIBILITIES OF UNDER SECRETARY.—Subject to the direction and control of the Secretary, the responsibilities of [the Under Secretary for Information Analysis and Infrastructure Protection] *the Under Secretary for Intelligence and Analysis* shall be as follows:

(1) * * *

[(2) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assess-

ments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).]

[(3) To integrate] *(2) To participate in the integration of* relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities.

[(4)] *(3)* To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this section, including obtaining such information from other agencies of the Federal Government.

[(5) To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency preparedness communications systems, and the physical and technological assets that support such systems.

[(6) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.]

[(7)] *(4)* To administer the Homeland Security Advisory System *under section 204*, including—

(A) * * *

* * * * * * *

[(8)] *(5)* To review, analyze, and make recommendations for improvements in the policies and procedures governing the sharing of law enforcement information, intelligence information, intelligence-related information, and other information relating to homeland security within the Federal Government and between the Federal Government and State and local government agencies and authorities.

[(9)] *(6)* To disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

[(10)] *(7)* To consult with the Director of Central Intelligence and other appropriate intelligence, law enforcement, or other elements of the Federal Government to establish collection priorities and strategies for information, including law enforcement-related information, relating to threats of terrorism

against the United States through such means as the representation of the Department in discussions regarding requirements and priorities in the collection of such information.

[(11)] *(8)* To consult with State and local governments and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

[(12)] *(9)* To ensure that—

(A) * * *

* * * * * * *

[(13)] *(10)* To request additional information from other agencies of the Federal Government, State and local government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

[(14)] *(11)* To establish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

[(15)] *(12)* To ensure, in conjunction with the chief information officer of the Department, that any information databases and analytical tools developed or utilized by the Department—

(A) * * *

* * * * * * *

[(16)] *(13)* To coordinate training and other support to the elements and personnel of the Department, other agencies of the Federal Government, and State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

[(17)] *(14)* To coordinate with *the Assistant Secretary for Infrastructure Protection and* elements of the intelligence community and with Federal, State, and local law enforcement agencies, and the private sector, as appropriate.

(15) To coordinate and enhance integration among intelligence components of the Department.

(16) To establish intelligence priorities, policies, processes, standards, guidelines, and procedures for the Department.

(17) To establish a structure and process to support the missions and goals of the intelligence components of the Department.

(18) To ensure that, whenever possible—

(A) the Under Secretary for Intelligence and Analysis produces and disseminates reports and analytic products based on open-source information that do not require a national security classification under applicable law; and

(B) such unclassified open-source reports are produced and disseminated contemporaneously with reports or analytic products concerning the same or similar information that the Under Secretary for Intelligence and Analysis produces and disseminates in a classified format.

(19) To establish within the Office of Intelligence and Analysis an Internal Continuity of Operations (COOP) Plan that—

(A) assures that the capability exists to continue uninterrupted operations during a wide range of potential emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies, that is maintained at a high level of readiness and is capable of implementation with and without warning; and

(B) includes plans and procedures governing succession to office within the Office of Intelligence and Analysis, including—

(i) emergency delegations of authority (where permissible, and in accordance with applicable law);

(ii) the safekeeping of vital resources, facilities, and records;

(iii) the improvisation or emergency acquisition of vital resources necessary for the performance of operations of the Office; and

(iv) the capability to relocate essential personnel and functions to and to sustain the performance of the operations of the Office at an alternate work site until normal operations can be resumed.

[(18)**]** *(20)* To provide intelligence and information analysis and support to other elements of the Department.

[(19)**]** *(21)* To perform such other duties relating to such responsibilities as the Secretary may provide.

[(e)**]** *(d)* STAFF.—

(1) IN GENERAL.—The Secretary shall provide the **[**Directorate**]** *Office* with a staff of analysts having appropriate expertise and experience to assist the **[**Directorate**]** *Office* in discharging responsibilities under this section.

* * * * * * *

[(f)**]** *(e)* DETAIL OF PERSONNEL.—

(1) IN GENERAL.—In order to assist the **[**Directorate**]** *Office* in discharging responsibilities under this section, personnel of the agencies referred to in paragraph (2) may be detailed to the Department for the performance of analytic functions and related duties.

* * * * * * *

[(g)**]** *(f)* FUNCTIONS TRANSFERRED.—In accordance with title XV, there shall be transferred to the Secretary, for assignment to **[**the Under Secretary for Information Analysis and Infrastructure Protection**]** *the Under Secretary for Intelligence and Analysis and the Assistant Secretary for Infrastructure Protection* under this section *and section 203*, the functions, personnel, assets, and liabilities of the following:

(1) * * *

* * * * * * *

SEC. 203. INTELLIGENCE COMPONENTS.

(a) RESPONSIBILITIES.—Subject to the direction and control of the Secretary, the responsibilities of the head of each intelligence component of the Department are as follows:

(1) To ensure that duties related to the acquisition, analysis, and dissemination of homeland security information are carried out effectively and efficiently in support of the Under Secretary for Intelligence and Analysis.

(2) To support and implement the goals established in cooperation with the Under Secretary for Intelligence and Analysis.

(3) To incorporate the input of the Under Secretary for Intelligence and Analysis with respect to performance appraisals, bonus or award recommendations, pay adjustments, and other forms of commendation.

(4) To coordinate with the Under Secretary for Intelligence and Analysis in the recruitment, establishment of core competency standards, and selection of intelligence officials of the intelligence component.

(5) To advise and coordinate with the Under Secretary for Intelligence and Analysis on any plan to reorganize or restructure the intelligence component that would, if implemented, result in realignments of intelligence functions.

(6) To ensure that employees of the intelligence component have knowledge of and comply with the programs and policies established by the Under Secretary for Intelligence and Analysis and other appropriate officials of the Department and that such employees comply with all applicable laws and regulations.

(7) To perform such other duties relating to such responsibilities as the Secretary may provide.

(b) TRAINING OF EMPLOYEES.—The Secretary shall provide training and guidance for employees, officials, and senior executives of the intelligence components of the Department to develop knowledge of laws, regulations, operations, policies, procedures, and programs that are related to the functions of the Department relating to the handling, analysis, dissemination, and collection of homeland security information.

SEC. 204. HOMELAND SECURITY ADVISORY SYSTEM.

(a) REQUIREMENT.—The Under Secretary for Intelligence and Analysis shall implement a Homeland Security Advisory System in accordance with this section to provide public advisories and alerts regarding threats to homeland security, including national, regional, local, and economic sector advisories and alerts, as appropriate.

(b) REQUIRED ELEMENTS.—The Under Secretary, in each advisory or alert issued under the System, shall—

(1) include information on appropriate protective measures and countermeasures that may be taken in response to the threat;

(2) whenever possible, limit the scope of the advisory or alert to a specific region, locality, or economic sector believed to be at risk; and

(3) not use color designations as the exclusive means of specifying the homeland security threat conditions that are the subject of the advisory or alert.

SEC. 205. HOMELAND SECURITY INFORMATION SHARING.

(a) INFORMATION SHARING ENVIRONMENT.—Consistent with section 1016 of the National Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), the Secretary shall integrate and standardize the information of the intelligence components of the Department into a Department information sharing environment, to be administered by the Under Secretary for Intelligence and Analysis.

(b) INFORMATION SHARING AND KNOWLEDGE MANAGEMENT OFFICERS.—For each intelligence component of the Department, the Secretary shall designate an information sharing and knowledge management officer who shall report to the Under Secretary for Intelligence and Analysis with respect to coordinating the different systems used in the Department to gather and disseminate homeland security information.

(c) STATE, LOCAL, TRIBAL, AND PRIVATE-SECTOR SOURCES OF INFORMATION.—

(1) ESTABLISHMENT OF BUSINESS PROCESSES.—The Under Secretary for Intelligence and Analysis shall establish Department-wide procedures for the review and analysis of information gathered from State, local, tribal, and private-sector sources and, as appropriate, integrate such information into the information gathered by the Department and other departments and agencies of the Federal Government.

(2) FEEDBACK.—The Secretary shall develop mechanisms to provide analytical and operational feedback to any State, local, tribal and private-sector entities that gather information and provide such information to the Secretary.

(d) TRAINING AND EVALUATION OF EMPLOYEES.—

(1) TRAINING.—The Under Secretary shall provide to employees of the Department opportunities for training and education to develop an understanding of the definition of homeland security information, how information available to them as part of their duties might qualify as homeland security information, and how information available to them is relevant to the Office of Intelligence and Analysis.

(2) EVALUATIONS.—The Under Secretary shall, on an ongoing basis, evaluate how employees of the Office of Intelligence and Analysis and the intelligence components of the Department are utilizing homeland security information and participating in the Department information sharing environment.

SEC. 206. COMPREHENSIVE INFORMATION TECHNOLOGY NETWORK ARCHITECTURE.

(a) ESTABLISHMENT.—The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall establish a comprehensive information technology network architecture for the Office of Intelligence and Analysis.

(b) NETWORK MODEL.—The comprehensive information technology network architecture established under subsection (a) shall, to the extent possible, incorporate the approaches, features, and functions of on the network proposed by the Markle Foundation in reports issued in October 2002 and December 2003, known as the System-wide Homeland Security Analysis and Resource Exchange (SHARE) Network.

(c) COMPREHENSIVE INFORMATION TECHNOLOGY NETWORK ARCHITECTURE DEFINED.—the term "comprehensive information technology network architecture" means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the strategic goals and information resources management goals of the Office of Intelligence and Analysis.

SEC. 207. STATE, LOCAL, TRIBAL, AND REGIONAL INFORMATION FUSION CENTER INITIATIVE.

(a) ESTABLISHMENT.—The Secretary shall establish a State, Local, and Tribal Information Fusion Center Initiative to establish partnerships with State, local, tribal, and regional information fusion centers.

(b) DUTIES.—Through the State, Local, Tribal, and Regional Information Fusion Center Initiative, the Secretary shall—

(1) coordinate with the principal official of each State, local, tribal, or regional information fusion center and the official designated as the Homeland Security Advisor of the State;

(2) provide Department operational and intelligence advice and assistance to State, local, tribal, and regional information fusion centers;

(3) support efforts to include State, local, tribal, and regional information fusion centers into efforts to establish an information sharing environment (as defined under section 1016(2) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458; 118 Stat. 3665));

(4) conduct table-top and live training exercises to regularly assess the capability of individual and regional networks of State, local, tribal, and regional information fusion centers to integrate the efforts of such networks with the efforts of the Department;

(5) coordinate with other relevant Federal entities engaged in homeland security-related activities;

(6) provide analytic and reporting advice and assistance to State, local, tribal, and regional information fusion centers;

(7) review homeland security information gathered by State, local, tribal, and regional information fusion centers and incorporate relevant information with homeland security information of the Department;

(8) Provide management assistance to State, local, tribal, and regional information fusion centers;

(9) Serve as a point of contact to ensure the dissemination of relevant homeland security information.

(10) facilitate close communication and coordination between State, local, tribal, and regional information fusion centers and the Department;

(11) provide State, local, tribal, and regional information fusion centers with expertise on Department resources and operations;

(12) provide training to State, local, tribal, and regional information fusion centers and encourage such information fusion centers to participate in terrorist threat-related exercises conducted by the Department; and

(13) carry out such other duties as the Secretary determines are appropriate.

(c) DEFINITION OF STATE, LOCAL, TRIBAL, OR REGIONAL INFORMATION FUSION CENTER.—For purposes of this section, the term "State, local, tribal, or regional information fusion center" means a local or regional center comprised of State, local, or tribal governmental entities that—

(1) serves as a data analysis and dissemination center for potentially relevant homeland security information;

(2) is managed by a state, local, or tribal government entity; or

(3) is designated as a State, local, tribal, or regional information fusion center by the Secretary.

SEC. 208. HOMELAND SECURITY INFORMATION SHARING FELLOWS PROGRAM.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Secretary, acting through the Under Secretary for Intelligence and Analysis, shall establish a fellowship program in accordance with this section for the purpose of—

(A) detailing State, local, and tribal analysts and law enforcement officials and officers to the Department to participate in the work of the Office of Intelligence and Analysis in order to become familiar with—

(i) the mission and capabilities of the Office of Intelligence and Analysis; and

(ii) the role, programs, products, and personnel of the Office of Intelligence and Analysis; and

(B) promoting information sharing between the Department and State, local, and tribal analysts and law enforcement agencies by stationing analysts and law enforcement officers alongside Department intelligence analysts in order to—

(i) serve as a point of contact in the Department to assist in the representation of State, local, and tribal homeland security information needs;

(ii) identify homeland security information of interest to State, local, and tribal analysts and law enforcement officers; and

(iii) assist Department analysts in preparing and disseminating terrorism-related products that are tailored to State, local, and tribal analysts and law enforcement agencies and designed to help thwart terrorist attacks.

(2) PROGRAM NAME.—The program under this section shall be known as the "Homeland Security Information Sharing Fellows Program".

(b) ELIGIBILITY.—

(1) IN GENERAL.—In order to be eligible for selection as an Information Sharing Fellow under the program, an individual must—

(A) have homeland security-related responsibilities or law enforcement-related responsibilities;

(B) be eligible for an appropriate national security clearance;

(C) possess a valid need for access to classified information, as determined by the Under Secretary for Intelligence and Analysis; and

(D) be an employee of an eligible entity.

(2) ELIGIBLE ENTITIES.—For purposes of this subsection, the term "eligible entity" means—

(A) a State, local, tribal, or regional fusion center;

(B) a State or local law enforcement or other government entity that serves a major metropolitan area, as determined by the Secretary;

(C) a State or local law enforcement or other government entity that serves a suburban or rural area, as determined by the Secretary;

(D) a State or local law enforcement or other government entity with port responsibilities, as determined by the Secretary;

(E) a State or local law enforcement or other government entity with border responsibilities, as determined by the Secretary;

(F) a State or local law enforcement or other government entity with agricultural responsibilities, as determined by the Secretary;

(G) a tribal law enforcement or other authority; or

(H) such other entity as the Secretary determines is appropriate.

(c) OPTIONAL PARTICIPATION.—No State, local, or tribal law enforcement or other government entity shall be required to participate in the Homeland Security Information Sharing Fellows Program.

(d) PROCEDURES FOR NOMINATION AND SELECTION.—

(1) IN GENERAL.—The Under Secretary shall establish procedures to provide for the nomination and selection of individuals to participate in the Homeland Security Information Sharing Fellows Program.

(2) LIMITATIONS.—The Under Secretary shall—

(A) select analysts and law enforcement officers representing a broad cross-section of State, local, and tribal agencies;

(B) ensure that the number of Information Sharing Fellows selected does not impede the activities of the Office of Intelligence and Analysis; and

(C) take reasonable steps to promote racial, ethnic, and gender diversity in the Information Sharing Fellows Program.

(e) LENGTH OF SERVICE.—Information Sharing Fellows shall serve for a reasonable period of time, as determined by the Under Secretary. Such period of time shall be sufficient to advance the information-sharing goals of the Under Secretary and encourage participation by as many qualified nominees as possible.

(f) CONDITION.—As a condition of selecting an individual as an Information Sharing Fellow under the program, the Under Secretary shall require that the individual's employer agree to continue to pay the individual's salary and benefits during the period for which the individual is detailed.

(g) STIPEND.—During the period for which an individual is detailed under the program, the Under Secretary shall, subject to the

availability of appropriations provide to the individual a stipend to cover the individual's reasonable living expenses for that period.

(h) SECURITY CLEARANCES.—If an individual selected for a fellowship under the Information Sharing Fellows Program does not possess the appropriate security clearance, the Under Secretary shall ensure that security clearance processing is expedited for such individual and shall ensure that each such Information Sharing Fellow has obtained the appropriate security clearance prior to participation in the Program.

SEC. 209. FULL AND EFFICIENT USE OF OPEN-SOURCE INTELLIGENCE.

(a) USE BY UNDER SECRETARY.—The Secretary shall ensure that, in meeting the analytic responsibilities under section 201(d) and in formulating requirements for additional information, the Under Secretary for Intelligence and Analysis makes full and efficient use of open-source information by acquiring, gathering, processing, and analyzing open-source information to produce open-source intelligence products.

(b) ANALYSIS PERFORMANCE.—The Secretary shall ensure that the Department makes full and efficient use of open-source information to analyze United States critical infrastructure nodes from the perspective of terrorists using publicly available information. The Secretary shall share the results of the analysis with appropriate Federal, State, local, tribal, and private-sector officials.

* * * * * * *

Subtitle C—Information Security

* * * * * * *

SEC. 223. ENHANCEMENT OF NON-FEDERAL CYBERSECURITY.

In carrying out the responsibilities under section 201, the [Under Secretary for Information Analysis and Infrastructure Protection] *Under Secretary for Intelligence and Analysis, in cooperation with the Assistant Secretary for Infrastructure Protection* shall—

(1) * * *

* * * * * * *

SEC. 224. NET GUARD.

The [Under Secretary for Information Analysis and Infrastructure Protection] *Assistant Secretary for Infrastructure Protection* may establish a national technology guard, to be known as "NET Guard", comprised of local teams of volunteers with expertise in relevant areas of science and technology, to assist local communities to respond and recover from attacks on information systems and communications networks.

* * * * * * *

Subtitle E—Infrastructure Protection and Cybersecurity

SEC. 241. OFFICE OF INFRASTRUCTURE PROTECTION.

(a) IN GENERAL.—There is in the Department an Office of Infrastructure Protection.

(b) ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION.—The head of the Office shall be the Assistant Secretary for Infrastructure Protection.

(c) RESPONSIBILITIES OF THE ASSISTANT SECRETARY.—The Assistant Secretary shall carry out the responsibilities of the Department regarding infrastructure protection. Such responsibilities shall include the following:

(1) To identify and carry out comprehensive risk assessments of key resources and critical infrastructure of the United States, to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

(2) To develop and maintain a comprehensive national plan for securing the key resources and critical infrastructure of the United States, in accordance with Homeland Security Presidential Directive 7.

(3) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Departments and agencies and in consultation with State, local, and tribal government agencies and authorities, and the private sector.

(4) To coordinate and implement, as appropriate, preparedness efforts to ensure that critical infrastructure and key resources efforts are fully integrated and coordinated with the response and recovery activities of the Department.

(5) To establish and maintain partnerships and information sharing processes with Federal, State, local, and tribal governments, the private sector, and international governments and organizations to enhance coordination of critical infrastructure and key resource efforts.

(6) To coordinate with the Under Secretary for Intelligence and Analysis and elements of the intelligence community and with Federal, State, local, and tribal law enforcement agencies, and the private sector, as appropriate.

(7) To provide the Secretary with an annual summary of national critical infrastructure protection efforts and priorities and to provide, in consultation with the appropriate Department official with primary responsibility for grants, recommendations for Federal critical infrastructure protection funding.

(8) In carrying out responsibilities under paragraphs (1) and (2), to consult with other Federal, State, local, and tribal government agencies and authorities as appropriate.

(9) To perform other such duties relating to such responsibilities as the Secretary may provide.

(d) INTEGRATION CENTER.—

(1) IN GENERAL.—There is an Integration Center in the Office of Infrastructure Protection, which shall be staffed by the Office of Infrastructure Protection, the Office of Cybersecurity and Telecommunications, and the Office of Intelligence and Analysis.

(2) RESPONSIBILITIES.—The Integration Center shall—

(A) be responsible for the integration of relevant threat, consequence, and vulnerability information, analysis, and assessments (whether such information, analysis, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other Federal departments and agencies, State, local, and tribal government agencies and authorities, the private sector, and other entities; and

(B) develop and disseminate analytical products that combine homeland security information with critical infrastructure and key resource vulnerability and consequence information.

(3) CRITICAL INFRASTRUCTURE INFORMATION.—The Secretary shall ensure that the Department makes full and efficient use of open-source information to analyze United States critical infrastructure from the perspective of terrorists using publicly available information.

(e) STAFF.—

(1) IN GENERAL.—The Secretary shall ensure that the Office has staff that possess appropriate expertise and experience to assist the Assistant Secretary in discharging responsibilities under this section.

(2) PRIVATE SECTOR STAFF.—Staff under this subsection may include individuals from the private sector.

(3) SECURITY CLEARANCES.—Staff under this subsection shall possess security clearances appropriate for their work under this section.

(f) DETAIL OF PERSONNEL.—

(1) IN GENERAL.—In order to assist the Office in discharging responsibilities under this section, personnel of other Federal departments and agencies may be detailed to the Department for the performance of analytic functions and related duties.

(2) COOPERATIVE AGREEMENTS.—The Secretary and the head of the Federal department or agency concerned may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

(3) BASIS.—The detail of personnel under this subsection may be on a reimbursable or non-reimbursable basis.

(g) REPROGRAMMING.—The Secretary may not reprogram any funds allocated to the Office of Infrastructure Protection until 60 days after the Secretary submits to the Committees on Appropriations of the Senate and House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives written notification of the reprogramming.

SEC. 242. OFFICE OF CYBERSECURITY AND TELECOMMUNICATIONS.

(a) IN GENERAL.—There is in the Department an Office of Cybersecurity and Telecommunications.

(b) ASSISTANT SECRETARY FOR CYBERSECURITY AND TELECOMMUNICATIONS.—The head of the Office shall be the Assistant Secretary for Cybersecurity and Telecommunications.

(c) RESPONSIBILITIES OF THE ASSISTANT SECRETARY.—The Assistant Secretary shall carry out the responsibilities of the Department regarding cybersecurity and telecommunications. Such responsibilities shall include the following:

(1) To establish and manage—

(A) a national cybersecurity response system that includes the ability to—

(i) analyze the effect of cybersecurity threat information on national critical infrastructure identified by the President; and

(ii) aid in the detection and warning of potential vulnerabilities or attacks that could cause widespread disruption of cybersecurity infrastructure and in the restoration of such infrastructure in the aftermath of such attacks;

(B) a national cybersecurity threat and vulnerability reduction program which conducts risk assessments on information technology systems, identifies and prioritize vulnerabilities in critical information infrastructure, and coordinates the mitigation of such vulnerabilities;

(C) an emergency communications program to ensure communications systems and procedures are in place to exchange information during disasters;

(D) a continuity of operations program to plan and allocate resources for the continuation of critical information operations in the event of a large scale disruption of the information infrastructure and to coordinate a response;

(E) a reconstitution program to ensure that priorities, procedures, and resources are in place to reconstitute critical information infrastructures. This program should clearly delineate roles and responsibilities of the Department, other federal agencies and private sector;

(F) a resiliency program that will support basic and fundamental research to improve the reliability and security of network protocols;

(G) a national public-private cybersecurity awareness, training, and education program that promotes Internet security awareness among all enduser groups;

(H) a government cybersecurity program to coordinate and consult with Federal, State, and local governments to enhance their cybersecurity programs; and

(I) an international cybersecurity cooperation program to help foster Federal efforts to enhance international cybersecurity awareness and cooperation.

(2) To coordinate and to leverage existing efforts within the private sector on the program under paragraph (1) as appropriate and to promote cybersecurity information sharing, vulnerability assessment, and threat warning regarding critical infrastructure.

(3) To coordinate with the Under Secretary for Intelligence and Analysis and the Assistant Secretary for Infrastructure Protection to provide relevant and timely homeland security in-

formation to the appropriate private sector information infrastructure stakeholders regarding potential vulnerabilities or attacks.

(4) To coordinate with other directorates and offices within the Department and with other Federal agencies, as appropriate, with respect to the cybersecurity aspects of such directorates, offices, and agencies.

(5) To coordinate with the Department official with primary responsibility for emergency preparedness to ensure that the National Response Plan developed includes appropriate measures for the recovery of the cybersecurity elements of critical infrastructure.

(6) To promote voluntary cybersecurity best practices, standards, and benchmarks that are responsive to rapid technology changes and to the security needs of critical infrastructure.

(7) To coordinate with the Chief Information Officer of the Department in establishing a secure information sharing architecture and information sharing processes, including with respect to the Department's operation centers.

(8) To consult with the Electronic Crimes Task Force of the United States Secret Service on private sector outreach and information activities.

(9) To consult with the appropriate Department official with primary responsibility for grants to ensure that realistic cybersecurity scenarios are incorporated into training exercises, including tabletop and recovery exercises.

(10) To consult and coordinate with the Assistant Secretary for Infrastructure Protection, the Under Secretary for Science and Technology, and, where appropriate, with other relevant Federal departments and agencies, as well as private sector stakeholders, on the security of digital control systems, such as Supervisory Control and Data Acquisition (SCADA) systems.

(11) To consult and coordinate with the Under Secretary of Science and Technology on cybersecurity research and development requirements.

(d) REPORTING.—Not later than one year after the date of the enactment of this section, the Secretary shall submit to Congress a report on the programs that implement or support the requirements of this section and the coordination of the Assistant Secretary with the private sector in meeting these responsibilities.

(e) DEADLINE FOR NOMINATION.—Not later than 90 days after the date of the enactment of this section, the President shall nominate an individual to serve as the Assistant Secretary for Cybersecurity and Telecommunications.

(f) STAFF.—

(1) IN GENERAL.—The Secretary shall provide the Office of Cybersecurity and Telecommunications with a staff having appropriate expertise and experience to assist the Assistant Secretary in discharging responsibilities under this section.

(2) SECURITY CLEARANCES.—Staff under this subsection shall possess security clearances appropriate for their work under this section.

(g) DETAIL OF PERSONNEL.—

(1) IN GENERAL.—In order to assist the Assistant Secretary for Cybersecurity and Telecommunications in discharging the

responsibilities of the Assistant Secretary under this section, personnel of other Federal departments and agencies may be detailed to the Department for the performance of analytic functions and related duties.

(2) COOPERATIVE AGREEMENTS.—The Secretary and the head of a Federal department or agency concerned may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

(3) BASIS.—The detail of personnel under this subsection may be on a reimbursable or non-reimbursable basis.

(h) REPROGRAMMING.—The Secretary may not reprogram any funds allocated to the Office of Cybersecurity and Telecommunications until 60 days after the Secretary submits to the Committees on Appropriations of the Senate and House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives written notification of the reprogramming.

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

SEC. 302. RESPONSIBILITIES AND AUTHORITIES OF THE UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY.

The Secretary, acting through the Under Secretary for Science and Technology, shall have the responsibility for—

(1) * * *

(2) developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for, identifying priorities, goals, objectives and policies for, and coordinating the Federal Government's civilian efforts to identify and develop countermeasures to chemical, biological**[**, radiological, nuclear**]**, and other emerging terrorist threats, including the development of comprehensive, research-based definable goals for such efforts and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts;

(3) supporting the **[**Under Secretary for Information Analysis and Infrastructure Protection**]** *Under Secretary for Intelligence and Analysis and the Assistant Secretary for Infrastructure Protection*, by assessing and testing homeland security vulnerabilities and possible threats;

* * * * * * *

(5) establishing priorities for, directing, funding, and conducting national research, development, test and evaluation, and procurement of technology and systems for—

(A) preventing the importation of chemical, biological**[**, radiological, nuclear**]**, and related weapons and material; and

* * * * * * *

SEC. 305. FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTERS.

The Secretary, acting through the Under Secretary for Science and Technology *and the Director of the Domestic Nuclear Detection Office*, shall have the authority to establish or contract with 1 or more federally funded research and development centers to provide independent analysis of homeland security issues, or to carry out other responsibilities under this Act, including coordinating and integrating both the extramural and intramural programs described in section 308.

* * * * * * *

SEC. 308. CONDUCT OF RESEARCH, DEVELOPMENT, DEMONSTRATION, TESTING AND EVALUATION.

(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology *and the Director of the Domestic Nuclear Detection Office*, shall carry out the responsibilities under section 302(4) through both extramural and intramural programs.

(b) EXTRAMURAL PROGRAMS.—

(1) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology *and the Director of the Domestic Nuclear Detection Office*, shall operate extramural research, development, demonstration, testing, and evaluation programs so as to—

(A) * * *

* * * * * * *

SEC. 311. HOMELAND SECURITY SCIENCE AND TECHNOLOGY ADVISORY COMMITTEE.

(a) * * *

* * * * * * *

[(j) TERMINATION.—The Department of Homeland Security Science and Technology Advisory Committee shall terminate 3 years after the effective date of this Act.**]**

(j) TERMINATION.—The Department of Homeland Security Science and Technology Advisory Committee shall terminate on the date that is 10 years after the date on which it was established.

* * * * * * *

TITLE IV—DIRECTORATE OF BORDER AND TRANSPORTATION SECURITY

* * * * * * *

Subtitle G—Transportation Security

SEC. 481. RAIL AND PUBLIC TRANSPORTATION VULNERABILITY ASSESSMENTS AND SECURITY PLANS.

(a) IN GENERAL.—

(1) REQUIREMENT.—Not later than 1 year after the date of enactment of this subtitle, the Secretary, acting through the Transportation Security Administration, shall promulgate regulations that—

(A) establish standards, protocols, and procedures for vulnerability assessments and security plans for rail and public transportation systems;

(B) require a designated rail or public transportation system owner or operator (as designated under subsection (b)) to—

(i) conduct an assessment of the vulnerability of the rail or public transportation system to an act of terrorism; and

(ii) prepare and implement a security plan that addresses the vulnerabilities identified in the vulnerability assessment; and

(C) set deadlines of no later than 2 years after the promulgation of the regulations for the completion of vulnerability assessments and security plans.

(2) CONSULTATION.—In promulgating the regulations under paragraph (1) the Secretary shall consult with the Department of Transportation and other appropriate Federal agencies.

(b) DESIGNATED RAIL OR PUBLIC TRANSPORTATION SYSTEM.—For the purposes of this subtitle, the term "designated rail or public transportation system" means—

(1) a heavy rail, light rail, commuter rail, or other freight or passenger rail system, including Federal and government sponsored entities;

(2) a ferry system; or

(3) an intracity or intercity bus system.

(c) VULNERABILITY ASSESSMENTS.—

(1) REQUIREMENTS.—For a rail or public transportation system designated under subsection (b), the Secretary shall provide assistance and guidance in conducting vulnerability assessments and shall require that the vulnerability assessments include at a minimum—

(A) identification and evaluation of critical infrastructure and assets, including subway platforms, rail, bus, and ferry terminals, rail tunnels, rail bridges, rail switching and storage areas, and information systems; and

(B) identification of vulnerabilities to the infrastructure and assets identified under subparagraph (A) in—

(i) physical security;

(ii) passenger and commuter security;

(iii) programmable electronic devices, computers, computer or communications networks, or other automated systems which are used by the rail or public transportation system;

(iv) alarms, cameras and other protection systems;

(v) communications systems;

(vi) utilities;

(vii) contingency response; and

(viii) other areas as determined by the Secretary.

(2) THREAT INFORMATION.—

(A) The vulnerability assessments under paragraph (1) shall incorporate any threat information as provided by the Secretary, and any other threat information relevant to the vulnerability of the rail or public transportation system.

(B) The Secretary shall provide in a timely manner, to the maximum extent practicable under applicable authority and in the interests of national security, to the rail or public transportation system subject to the requirements in paragraph (1), threat information that is relevant to that rail or public transportation system, including an assessment of the most likely method that could be used by terrorists to exploit vulnerabilities, and their likelihood of success.

(d) SECURITY PLANS.—

(1) REQUIREMENTS.—For a rail or public transportation system designated under subsection (b), the Secretary shall provide assistance and guidance in preparing and implementing security plans and shall require that the security plan include at a minimum—

(A) security measures to address the vulnerabilities identified in the vulnerability assessment required under subsection (c);

(B) plans for periodic drills and exercises that include participation by local law enforcement agencies and first responders as appropriate;

(C) equipment, plans, and procedures to be implemented or used by the rail or public transportation system in response to a terrorist attack, including evacuation and passenger communication plans;

(D) identification of steps taken with State and local law enforcement agencies, first responders, and Federal officials to coordinate security measures and plans for response to a terrorist attack;

(E) a description of training and exercises for employees of a rail or public transportation system, which includes, as appropriate, a strategy or timeline for training;

(F) enhanced security measures to be taken when the Secretary declares a period of heightened security risk; and

(G) other actions or procedures the Secretary determines are appropriate to address the vulnerability of a rail or public transportation system to a terrorist attack.

(2) CONSISTENCY WITH OTHER PLANS.—Security plans shall be consistent with the requirements of the National Infrastructure Protection Plan (including any Transportation Sector Specific Plan) and the National Strategy for Transportation Security.

(e) EXISTING PROCEDURES, PROTOCOLS, AND STANDARDS.—

(1) DETERMINATION.—In response to a petition by a person, or at the discretion of the Secretary, the Secretary may endorse or recognize existing procedures, protocols, and standards that the Secretary determines to meet all or part of the requirements of this subtitle regarding vulnerability assessments and security plans.

(2) REQUIREMENTS.—Upon review and written determination by the Secretary that existing procedures, protocols, or standards for a rail or public transportation system satisfy some or all of the requirements of this subtitle, any rail or public transportation system may elect to comply with those procedures, protocols, or standards.

(3) PARTIAL APPROVAL.—If the Secretary finds that the existing procedures, protocols, and standards satisfy only part of the requirements of this subtitle, he may accept those submissions, but shall require submission of any additional information relevant to vulnerability assessments and security plans to ensure that the requirements of this subtitle are fulfilled.

(4) NOTIFICATION.—If the Secretary does not endorse or recognize particular procedures, protocols, and standards, the Secretary shall provide to each person that submitted a petition under paragraph (1) a written notification that includes an explanation of the reasons why the endorsement or recognition was not made.

(f) CO-LOCATED FACILITIES.—The Secretary shall permit the development and implementation of coordinated vulnerability assessments and security plans, at the discretion of a rail or public transportation system owner or operator, to the extent two or more rail or public transportation systems have shared facilities, such as tunnels, bridges, or stations, or facilities that are geographically close or otherwise co-located.

(g) ENFORCEMENT.—Regulations promulgated under this section may be enforced by the Secretary through penalties authorized under section 114(u) of title 49, United States Code.

SEC. 482. NATIONAL RAIL AND PUBLIC TRANSPORTATION SECURITY PLAN.

(a) IN GENERAL.—The Secretary shall develop and implement, and update as appropriate, a supplement to the National Strategy for Transportation Security required under section 114(t) of title 49, United States Code to be entitled the "National Rail and Public Transportation Security Plan".

(b) INCLUDED ELEMENTS.—The supplement required under subsection (a) shall—

(1) include a description of the roles, responsibilities, and authorities of Federal, State, and local agencies, designated Federal and government sponsored entities, tribal governments, and appropriate rail and public transportation stakeholders, including nonprofit employee organizations that represent rail and public transportation system employees;

(2) identify and address gaps and unnecessary overlaps in the roles, responsibilities, or authorities described in paragraph (1);

(3) identify and make recommendations regarding legislative, regulatory, and organizational changes necessary to improve coordination among the entities described in paragraph (1) to enhance the security of rail and public transportation systems;

(4) provide measurable goals, including objectives, mechanisms and a schedule, for enhancing the security of rail and public transportation systems;

(5) include a process for sharing intelligence and information with the entities described in paragraph (1);

(6) include a process for expediting security clearances to facilitate intelligence and information sharing with the entities described in paragraph (1);

(7) describe current and future public outreach and educational initiatives designed to inform the public how to prevent, prepare for and respond to a terrorist attack on rail and public transportation systems;

(8) include a framework for resuming the operation of rail and public transportation systems as soon as possible in the event of an act of terrorism;

(9) include a strategy and timeline for the Department and other appropriate Federal agencies to research and develop new technologies, including advanced technologies with long term research and development timelines for securing rail and public transportation systems;

(10) build on available resources and consider costs and benefits;

(11) describe how the Department has reviewed the previous attacks on rail and public transportation systems throughout the world in the last 10 years, the lessons learned from this review, and how these lessons inform current and future efforts to secure rail and public transportation systems; and

(12) expand upon, leverage, and relate to existing strategies and plans, including the National Infrastructure Protection Plan required by Homeland Security Presidential Directive-7.

SEC. 483. RAIL AND PUBLIC TRANSPORTATION STRATEGIC INFORMATION SHARING PLAN.

(a) IN GENERAL.—The Secretary, in consultation with the Secretary of Transportation, shall develop and submit to the appropriate congressional committees no later than 90 days after the enactment of this subtitle a Rail and Public Transportation Strategic Information Sharing Plan to ensure the robust development of both tactical and strategic intelligence products pertaining to the threats and vulnerabilities to rail and public transportation systems for dissemination to Federal, State, and local agencies; tribal governments; and appropriate rail and public transportation stakeholders.

(b) CONTENT OF PLAN.—The plan required under subsection (a) shall include—

(1) a description of how intelligence analysts in the Transportation Security Administration are coordinating with other intelligence analysts in the Department and other Federal, State, and local agencies;

(2) deadlines for the completion of any organizational changes within the Department to accommodate implementation of the plan; and

(3) a description of resource needs for fulfilling the plan.

(c) UPDATES.—

(1) After the plan is provided under subsection (a), the Secretary shall certify to the appropriate congressional committees when the plan has been fully implemented.

(2) After the Secretary provides the certification under paragraph (1), the Secretary shall provide a report to the appropriate congressional committees each year thereafter on the following:

(A) The number and brief description of each rail and public transportation intelligence report created and disseminated under the plan.

(B) The classification of each report as tactical or strategic.

(C) The numbers of different government, law enforcement, and private sector partners who were provided with each intelligence product.

SEC. 484. PASSENGER IDENTIFICATION DOCUMENTS.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this section, the Assistant Secretary of Homeland Security (Transportation Security Administration) shall issue regulations to require a passenger to present an acceptable personal identification document for inspection before entering a sterile area of an airport in the United States. Such inspections shall be carried out by personnel designated by the Assistant Secretary.

(b) ACCEPTABLE PERSONAL IDENTIFICATION DOCUMENTS.—

(1) IN GENERAL.—In carrying out subsection (a), the Assistant Secretary shall establish a list of acceptable personal identification documents.

(2) MINIMUM REQUIREMENTS.—The Assistant Secretary may include a personal identification document on the list to be established under paragraph (1) only if the document is issued under the authority of the United States Government, a State, or a foreign government and includes each of the following:

(A) The individual's full legal name.

(B) The individual's date of birth.

(C) The individual's gender.

(D) A photograph of the individual.

(E) The individual's signature.

(F) Physical security features designed to prevent tampering, counterfeiting, and duplication of the document for fraudulent purposes.

(3) DRIVERS' LICENSES AND PERSONAL IDENTIFICATION CARDS.—The Assistant Secretary shall include on the list to be established under paragraph (1) drivers' licenses and personal identification cards that meet the requirements of section 202 of the Real ID Act of 2005 (49 U.S.C. 30301 note).

(c) PROCEDURES AND STANDARDS.—In carrying out subsection (a), the Assistant Secretary shall establish—

(1) procedures to match the name on a personal identification document with the name on an airline boarding document;

(2) procedures to match the photograph on a personal identification document with the passenger presenting the document; and

(3) standards for training personnel who check personal identification documents to recognize unacceptable and false identification documents.

(d) FAILURE TO PRESENT ACCEPTABLE IDENTIFICATION DOCUMENTS.—A passenger attempting to enter a sterile area of an airport in the United States who does not present an acceptable identification document shall be subject to such additional security screening as the Assistant Secretary determines to be appropriate before the passenger may be admitted to the sterile area.

(e) KNOWING PRESENTATION OF FALSE IDENTIFICATION DOCUMENTS; PENALTIES.—A passenger who knowingly presents a false identification document in an attempt to enter a sterile area of an airport in the United States shall be fined under title 18, United States Code, imprisoned for not more than 5 years, or both.

(f) DEFINITIONS.—In this section, the following definitions apply:

(1) FALSE.—The term "false" has the meaning given such term by section 1028(d) of title 18, United States Code.

(2) PASSENGER.—The term "passenger" means an individual to be carried aboard a passenger aircraft to be operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation (as such terms are defined in section 40102 of title 49, United States Code).

(3) STERILE AREA.—The term "sterile area" means any part of an airport that is regularly accessible to passengers after having cleared a passenger security checkpoint.

TITLE V—EMERGENCY PREPAREDNESS AND RESPONSE

* * * * * * *

SEC. 502. RESPONSIBILITIES.

(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Emergency Preparedness and Response, shall include—

(1) * * *

* * * * * * *

(b) COORDINATOR FOR ISSUES RELATING TO INDIVIDUALS WITH DISABILITIES.—The Under Secretary for Preparedness shall appoint a coordinator for issues relating to individuals with disabilities. Such individual shall report to the Under Secretary and to the Officer for Civil Rights and Civil Liberties.

* * * * * * *

SEC. 507. ROLE OF FEDERAL EMERGENCY MANAGEMENT AGENCY.

(a) * * *

* * * * * * *

(c) COORDINATOR FOR ISSUES RELATING TO INDIVIDUALS WITH DISABILITIES.—The Director of the Federal Emergency Management Agency shall appoint an individual to serve as the Director's coordinator for issues relating to individuals with disabilities. Such individual shall report to the Director and to the Officer for Civil Rights and Civil Liberties.

* * * * * * *

SEC. 510. PROCUREMENT OF SECURITY COUNTERMEASURES FOR STRATEGIC NATIONAL STOCKPILE.

(a) * * *

* * * * * * *

(d) RELATED AUTHORIZATIONS OF APPROPRIATIONS.—

(1) THREAT ASSESSMENT CAPABILITIES.—For the purpose of carrying out the responsibilities of the Secretary for terror threat assessment under the security countermeasures program, there are authorized to be appropriated such sums as may be necessary for each of the fiscal years 2004 through ⟦2006,⟧ *2009,* for the hiring of professional personnel within the ⟦Directorate for Information Analysis and Infrastructure Protection⟧ *Office of Intelligence and Analysis*, who shall be analysts responsible for chemical, biological, radiological, and nuclear threat assessment (including but not limited to analysis of chemical, biological, radiological, and nuclear agents, the

means by which such agents could be weaponized or used in a terrorist attack, and the capabilities, plans, and intentions of terrorists and other non-state actors who may have or acquire such agents). All such analysts shall meet the applicable standards and qualifications for the performance of intelligence activities promulgated by the Director of Central Intelligence pursuant to section 104 of the National Security Act of 1947.

(2) INTELLIGENCE SHARING INFRASTRUCTURE.—For the purpose of carrying out the acquisition and deployment of secure facilities (including information technology and physical infrastructure, whether mobile and temporary, or permanent) sufficient to permit the Secretary to receive, not later than 180 days after the date of enactment of the Project BioShield Act of 2004, all classified information and products to which the [Under Secretary for Information Analysis and Infrastructure Protection] *Under Secretary for Intelligence and Analysis* is entitled under subtitle A of title II, there are authorized to be appropriated such sums as may be necessary for each of the fiscal years 2004 through 2006.

(3) ADDITIONAL AUTHORIZATION OF APPROPRIATIONS REGARDING CERTAIN THREAT ASSESSMENTS.—For the purpose of providing an additional amount to the Secretary to assist the Secretary in meeting the requirements of clause (iv) of section 319F–2(c)(2)(A)) of the Public Health Service Act (relating to time frames), there are authorized to be appropriated such sums as may be necessary for fiscal year 2007, in addition to the authorization of appropriations established in paragraph (1). The purposes for which such additional amount may be expended include conducting risk assessments regarding clause (i)(II) of such section when there are no existing risk assessments that the Secretary considers credible.

SEC. [510] *511.* URBAN AND OTHER HIGH RISK AREA COMMUNICATIONS CAPABILITIES.

(a) * * *

* * * * * * *

SEC. 512. CONTRACTS FOR ASSISTANCE ACTIVITIES RELATING TO ACTS OF TERRORISM, NATURAL DISASTERS, AND OTHER EMERGENCIES.

(a) USE OF LOCAL FIRMS.—In entering into contracts and other agreements for debris clearance, distribution of supplies, reconstruction, and other assistance activities relating to an act of terrorism, natural disaster, or other emergency, the Secretary or the head of any component of the Department shall work toward a goal of awarding not less than 20 percent of the total value of the contracts and other agreements to qualified firms located in a county, parish, or equivalent division of general local government within the affected area.

(b) LIMITATION.—A goal established under this section shall apply only to the extent that the goal does not interfere with the ability of the Department to provide timely and effective assistance.

(c) PREFERENCE FOR SMALL BUSINESS CONCERNS.—In entering into contracts and other agreements described in subsection (a), the Secretary or the head of any component of the Department shall give preference to small business concerns, socially and economically dis-

advantaged small business concerns, small business concerns owned and controlled by service-disabled veterans, and HUBZone small business concerns (as those terms are defined in the Small Business Act (15 U.S.C. 631 et seq.)).

(d) PRENEGOTIATED CONTRACTS.—In order to increase the use of local firms in contracts and other agreements described in subsection (a), the Secretary shall encourage the components of the Department, as well as appropriate State and local government agencies, to competitively bid and negotiate contracts and prices for services, including debris clearance, distribution of supplies, reconstruction, and other assistance, in advance of an act of terrorism, natural disaster, or other emergency.

SEC. 513. CHIEF MEDICAL OFFICER.

(a) IN GENERAL.—There is in the Department a Chief Medical Officer, who shall be appointed by the President, by and with the advice and consent of the Senate.

(b) QUALIFICATIONS.—The individual appointed as Chief Medical Officer shall possess a demonstrated ability in and knowledge of medicine and public health.

(c) RESPONSIBILITIES.—The Chief Medical Officer shall have the primary responsibility within the Department for medical issues related to acts of terrorism, natural disasters, and other emergencies, including the following:

(1) Serving as the Secretary's principal advisor on medical and public health issues.

(2) Coordinating the biosurveillance and detection activities of the Department.

(3) Ensuring that decision support tools link biosurveillance and detection information to near real-time response actions at the State, local, and tribal level.

(4) Ensuring internal and external coordination of all medical preparedness and response activities of the Department, including training, exercises, and equipment support.

(5) Serving as the Department's primary point of contact on medical and public health issues with the Departments of Agriculture, Defense, Health and Human Services, Transportation, and Veterans Affairs, and other Federal departments or agencies.

(6) Serving as the Department's primary point of contact with respect to medical and public health matters.

(7) Discharging, in coordination with the Under Secretary for Science and Technology, responsibilities of the Department related to Project Bioshield.

(8) Establishing doctrine and priorities for the National Disaster Medical System and supervising its medical components, consistent with the National Response Plan and the National Incident Management System.

(9) Establishing doctrine and priorities for the Metropolitan Medical Response System, consistent with the National Response Plan and the National Incident Management System.

(10) Assessing the capability of the Department to contribute to enhancing the national medical surge capacity to respond to acts of terrorism, natural disasters, and other emergencies.

(11) Performing such other duties relating to such responsibilities as the Secretary may require.

(d) DEPUTY.—There is in the Department a Deputy Chief Medical Officer, who shall be appointed by the Secretary and who shall assist the Chief Medical Officer in carrying out the responsibilities under subsection (c).

SEC. 514. RAIL AND PUBLIC TRANSPORTATION SECURITY GRANT PROGRAM.

(a) GRANTS AUTHORIZED.—The Secretary, acting through the Department official with primary responsibility for grants and training, shall establish a grant program to allocate Federal homeland security assistance administered by the Department to United States rail and public transportation systems designated under section 481 on the basis of risk and need.

(b) PRIORITIZATION PROCESS.—In awarding grants under this section, the Secretary shall conduct an assessment of United States rail and public transportation systems to develop a prioritization for awarding grants authorized under subsection (a) based upon—

(1) the most current risk assessment available from the Department, incorporating threat, vulnerability, and consequence analysis;

(2) the national economic and strategic defense considerations of individual rail and public transportation systems; and

(3) any other factors that the Secretary determines to be appropriate.

(c) APPLICATION.—

(1) IN GENERAL.—Any rail or public transportation security system subject to the requirements of section 481 may submit an application for a grant under this section, at such time, in such form, and containing such information and assurances as the Secretary may require.

(2) MINIMUM STANDARDS FOR PAYMENT OR REIMBURSEMENT.—Each application submitted under paragraph (1) shall include—

(A) a comprehensive description of—

(i) the purpose of the project for which the applicant seeks a grant under this section and why the applicant needs the grant;

(ii) the applicability of the project to the security plan prepared under section 481 and other homeland security plans;

(iii) any existing cooperation or mutual aid agreements with other rail or public transportation systems, organizations, or State, and local governments as such agreements relate to rail and public transportation security; and

(iv) a capital budget showing how the applicant intends to allocate and expend the grant funds; and

(B) a determination by the Transportation Security Administration that the project—

(i) addresses or corrects rail and public transportation security vulnerabilities; and

(ii) helps to ensure compliance with the security plan prepared under section 481.

(3) PROCEDURAL SAFEGUARDS.—The Secretary, in consultation with the Office of the Inspector General and the Department official with primary responsibility for grants and train-

ing, shall issue guidelines to establish appropriate accounting, reporting, and review procedures to ensure that—

(A) grant funds are used for the purposes for which they were made available;

(B) grantees have properly accounted for all expenditures of grant funds; and

(C) grant funds not used for such purposes and amounts not obligated or expended are returned.

(d) USE OF FUNDS.—Grants awarded under this section may be used—

(1) to help implement security plans prepared under section 481;

(2) to remedy rail and public transportation security vulnerabilities identified through vulnerability assessments approved by the Secretary;

(3) for non-Federal projects contributing to the overall security of a rail or public transportation security system, as determined by the Secretary;

(4) for the salaries, benefits, overtime compensation, and other costs of additional security personnel for State and local agencies for activities required by the security plan prepared under section 481;

(5) for the cost of acquisition, operation, and maintenance of equipment that contributes to the overall security of the rail and public transportation security system, if the need is based upon vulnerability assessments approved by the Secretary or identified in a security plan prepared under section 481;

(6) to conduct vulnerability assessments approved by the Secretary;

(7) to purchase or upgrade equipment, including communications equipment that is interoperable with Federal, State, and local agencies and tribal governments; and computer software, to enhance terrorism preparedness;

(8) to conduct exercises or training for prevention and detection of, preparedness for, response to, or recovery from acts of terrorism;

(9) to establish or enhance mechanisms for sharing terrorism threat information and to ensure that the mechanisms are interoperable with Federal, State, and local agencies and tribal governments;

(10) for the cost of equipment (including software) required to receive, transmit, handle, and store classified information; and

(11) for the protection of critical infrastructure against potential attack by the addition of barriers, fences, gates, and other such devices, except that the cost of such measures may not exceed the greater of—

(A) $1,000,000 per project; or

(B) such greater amount as may be approved by the Secretary, which may not exceed 10 percent of the total amount of the grant.

(e) REIMBURSEMENT OF COSTS.—An applicant for a grant under this section may petition the Secretary for the reimbursement of the cost of any activity relating to prevention (including detection) of, preparedness for, response to, or recovery from acts of terrorism that is a Federal duty and usually performed by a Federal agency, and

that is being performed by a State or local government (or both) under agreement with a Federal agency.

(f) PROHIBITED USES.—Grants awarded under this section may not be used to—

(1) supplant State or local funds for activities of the type described in subsection (d);

(2) to construct buildings or other physical facilities, including barriers, fences, gates, and other such devices intended for the protection of critical infrastructure against potential attack, except those that are constructed under terms and conditions consistent with the requirements of section 611(j)(8) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5196(j)(8)), and the cost of which does not exceed the greater of—

(A) $1,000,000 per project; or

(B) such greater amount as may be approved by the Secretary, which may not exceed 10 percent of the total amount of the covered grant;

(3) acquire land; or

(4) make any State or local government cost-sharing contribution.

(g) MATCHING REQUIREMENT.—

(1) IN GENERAL.—Except as provided in subparagraph (A) or (B) of paragraph (2), Federal funds for any eligible project under this section shall not exceed 75 percent of the total cost of such project.

(2) EXCEPTIONS.—

(A) SMALL PROJECTS.—The requirement of paragraph (1) shall not apply with respect to a project with a total cost of not more than $25,000.

(B) HIGHER LEVEL OF FEDERAL SUPPORT REQUIRED.—The requirement of paragraph (1) shall not apply with respect to a project if the Secretary determines that the project merits support and cannot be undertaken without a higher rate of Federal support than the rate described in paragraph (1).

(3) IN-KIND CONTRIBUTIONS.—Each recipient of a grant under this section may meet the requirement of paragraph (1) by making in-kind contributions of goods or services that are directly linked with the purpose for which the grant is made, as determined by the Secretary, including any necessary personnel expenses, contractor services, administrative costs, equipment, fuel, or maintenance, and rental space.

(h) MULTIPLE PHASE PROJECTS.—

(1) IN GENERAL.—The Secretary may award grants under this section for projects that span multiple years.

(2) FUNDING LIMITATION.—Not more than 20 percent of the total grant funds awarded under this section in any fiscal year may be awarded for projects that span multiple years.

(i) CONSISTENCY WITH PLANS.—The Secretary shall ensure that each grant awarded under this section—

(1) is used to supplement and support, in a consistent and coordinated manner, the applicable security plan; and

(2) is consistent and coordinated with any applicable State or Urban Area Homeland Security Plan.

(j) COORDINATION AND COOPERATION.—The Secretary shall ensure that all projects that receive grant funding under this section within any area defined in an Urban Area Homeland Security Plan are coordinated with other projects in such area.

(k) REVIEW AND AUDITS.—The Secretary shall require all grantees under this section to maintain such records as the Secretary may require and make such records available for review and audit by the Secretary, the Comptroller General of the United States, or the Inspector General of the Department.

(l) QUARTERLY REPORTS REQUIRED AS A CONDITION OF HOMELAND SECURITY GRANTS.—

(1) EXPENDITURE REPORTS REQUIRED.—As a condition of receiving a grant under this section, the Secretary shall require the grant recipient to submit quarterly reports to the Secretary that describe each expenditure made by the recipient using grant funds.

(2) DEADLINE FOR REPORTS.—Each report required under paragraph (1) shall be submitted not later than 30 days after the last day of a fiscal quarter and shall describe expenditures made during that fiscal quarter.

(3) PUBLICATION OF EXPENDITURES.—

(A) IN GENERAL.—Not later than 1 week after receiving a report under this subsection, the Secretary shall publish and make publicly available on the Internet website of the Department a description of each expenditure described in the report.

(B) WAIVER.—The Secretary may waive the requirement of subparagraph (A) if the Secretary determines that it is in the national security interests of the United States to do so.

TITLE VI—POLICY, PLANNING, AND INTERNATIONAL AFFAIRS

SEC. 601. DIRECTORATE FOR POLICY, PLANNING, AND INTERNATIONAL AFFAIRS.

(a) ESTABLISHMENT.—There is in the Department a Directorate for Policy, Planning, and International Affairs.

(b) UNDER SECRETARY FOR POLICY.—

(1) IN GENERAL.—The head of the Directorate is the Under Secretary for Policy, who shall be appointed by the President.

(2) QUALIFICATIONS.—No individual shall be appointed Under Secretary for Policy under paragraph (1) unless the individual has, by education and experience, demonstrated knowledge, ability, and skill in the fields of policy and strategic planning.

(c) RESPONSIBILITIES OF UNDER SECRETARY.—

(1) POLICY RESPONSIBILITIES.—Subject to the direction and control of the Secretary, the policy responsibilities of the Under Secretary for Policy shall be as follows:

(A) To serve as the principal policy advisor to the Secretary.

(B) To provide overall direction and supervision of policy development for the programs, offices, and activities of the Department.

(C) To establish and implement a formal policymaking process for the Department.

(D) To analyze, evaluate, and review the completed, ongoing, and proposed programs of the Department to ensure they are compatible with the statutory and regulatory responsibilities of the Department and with the Secretary's priorities, strategic plans, and policies.

(E) To ensure that the budget of the Department (including the development of future year budgets and interaction with the Office of Management and Budget and with Congress) is compatible with the statutory and regulatory responsibilities of the Department and with the Secretary's priorities, strategic plans, and policies.

(F) To represent the Department in any development of policy that requires the Department to consult with another Federal agency, the Office of the President, a foreign government, or any other governmental or private sector entity.

(G) To supervise and oversee policy development undertaken by the component agencies and offices of the Department.

(H) To provide for the coordination and maintenance of the trade and customs revenue functions of the Department.

(2) STRATEGIC PLANNING RESPONSIBILITIES.—Subject to the direction and control of the Secretary, the strategic planning responsibilities of the Under Secretary for Policy shall be as follows:

(A) To conduct long-range, strategic planning for the Department.

(B) To prepare national and Department strategies, as appropriate.

(C) To conduct net assessments of issues facing the Department.

(3) INTERNATIONAL RESPONSIBILITIES.—Subject to the direction and control of the Secretary, the international responsibilities of the Under Secretary for Policy shall be as follows:

(A) To promote the exchange of information and the sharing of best practices and technology relating to homeland security with nations friendly to the United States, including—

(i) the exchange of information on research and development on homeland security technologies in coordination with the Under Secretary for Science and Technology;

(ii) joint training exercises of first responders in coordination with the Department official with primary responsibility for grants and training; and

(iii) exchanging expertise and information on terrorism prevention, response, and crisis management in coordination with the Director of the Federal Emergency Management Agency.

(B) To identify any homeland security-related area in which the United States and other nations and appropriate

international organizations could collaborate to improve capabilities and to encourage the exchange of information or sharing of best practices and technology relating to that area.

(C) To plan and participate in international conferences, exchange programs (including the exchange of scientists, engineers, and other experts), and other training activities with friendly nations in coordination with the Under Secretary for Science and Technology.

(D) To manage international activities within the Department in coordination with other Federal officials with responsibility for counterterrorism matters.

(E) To oversee the activities of Department personnel operating in other countries or traveling to other countries.

(F) To represent the Department in international negotiations and working groups.

(4) PRIVATE SECTOR.—

(A) To create and foster strategic communications with the private sector to enhance the primary mission of the Department to protect the United States.

(B) To advise the Secretary on the impact on the private sector of the policies, regulations, processes, and actions of the Department.

(C) To create and manage private sector advisory councils composed of representatives of industries and associations designated by the Secretary—

(i) to advise the Secretary on private sector products, applications, and solutions as they relate to homeland security challenges; and

(ii) to advise the Secretary on homeland security policies, regulations, processes, and actions that affect the participating industries and associations.

(D) To promote existing public-private partnerships and develop new public-private partnerships to provide for collaboration and mutual support to address homeland security challenges.

(E) To identify private sector resources and capabilities that could be effective in supplementing functions of the Department and State and local governments to prevent or respond to acts of terrorism.

(F) To coordinate among the Department's operating entities and with the Assistant Secretary for Trade Development of the Department of Commerce on issues related to the travel and tourism industries.

(5) TRADE AND CUSTOMS REVENUE FUNCTIONS.—The Under Secretary for Policy shall—

(A) ensure that the trade and customs revenue functions of the Department are coordinated within the Department and with other Federal departments and agencies, and that the impact on legitimate trade is taken into account in any action impacting these functions; and

(B) monitor and report to Congress on the Department's mandate to ensure that the trade and customs revenue functions of the Department are not diminished, including how spending, operations, and personnel related to these

functions have kept pace with the level of trade entering the United States.

SEC. 602. OFFICE OF INTERNATIONAL AFFAIRS.

(a) ESTABLISHMENT.— There is established within the Directorate of Policy, Planning, and International Affairs an Office of International Affairs. The Office shall be headed by an Assistant Secretary, who shall be appointed by the Secretary.

(b) DUTIES OF THE ASSISTANT SECRETARY.—The Assistant Secretary for International Affairs, in coordination with the Under Secretary for Science and Technology, the Director of the Federal Emergency Management Agency, the Department official with primary responsibility for grants and training, and other officials of the Department, as appropriate, shall have the following duties:

(1) To promote information and education exchange with nations friendly to the United States in order to promote sharing of best practices and technologies relating to homeland security. Such exchange shall include the following:

(A) Exchange of information on research and development on homeland security technologies.

(B) Joint training exercises of first responders.

(C) Exchange of expertise on terrorism prevention, response, and crisis management.

(2) To identify areas for homeland security information and training exchange where the United States has a demonstrated weakness and another friendly nation or nations have a demonstrated expertise.

(3) To plan and undertake international conferences, exchange programs, and training activities.

(4) To manage international activities within the Department in coordination with other Federal officials with responsibility for counter-terrorism matters.

SEC. 603. OTHER OFFICES AND OFFICIALS.

(a) IN GENERAL.—The Under Secretary for Policy shall establish the following offices in the Directorate for Policy, Planning, and International Affairs:

(1) The Office of Policy, which shall be administered by an Assistant Secretary for Policy.

(2) The Office of Strategic Plans, which shall be administered by an Assistant Secretary for Strategic Plans and which shall include—

(A) a Secure Border Initiative Program Office; and

(B) a Screening Coordination and Operations Office.

(3) The Office of the Private Sector, which shall be administered by an Assistant Secretary for the Private Sector.

(4) The Victim Assistance Officer.

(5) The Tribal Security Officer.

(6) Such other offices as considered necessary by the Under Secretary for Policy.

(b) DIRECTOR OF CARGO SECURITY POLICY.—

(1) IN GENERAL.—There shall be in the Directorate for Policy, Planning, and International Affairs a Director of Cargo Security Policy (hereinafter in this subsection referred to as the "Director"), who shall be subject to the direction and control of the Under Secretary for Policy.

(2) RESPONSIBILITIES.—The Director shall—

(A) advise the Assistant Secretary for Policy regarding all aspects of Department programs relating to cargo security;

(B) develop Department-wide policies regarding cargo security; and

(C) coordinate the cargo security policies and programs of the Department with other Federal departments and agencies, including by working with officials of the Department of Energy and the Department of State, as appropriate, in negotiating international agreements relating to cargo security.

(c) DIRECTOR OF TRADE POLICY.—

(1) IN GENERAL.—There shall be in the Directorate for Policy, Planning, and International Affairs a Director of Trade Policy (hereinafter in this subsection referred to as the "Director"), who shall be subject to the direction and control of the Under Secretary for Policy.

(2) RESPONSIBILITIES.—The Director shall—

(A) advise the Assistant Secretary for Policy regarding all aspects of Department programs relating to the trade and customs revenue functions of the Department;

(B) develop Department-wide policies regarding trade and customs revenue functions and trade facilitation; and

(C) coordinate the trade and customs revenue-related programs of the Department with other Federal departments and agencies.

SEC. 604. CONSULTATION ON TRADE AND CUSTOMS REVENUE FUNCTIONS.

(a) IN GENERAL.—The Secretary and the Under Secretary for Policy shall consult with representatives of the business community involved in international trade, including seeking the advice and recommendations of the Commercial Operations Advisory Committee (COAC), on Department policies and actions that have a significant impact on international trade and customs revenue functions.

(b) COAC CONSULTATION AND NOTIFICATION.—

(1) IN GENERAL.—Subject to paragraph (2), the Secretary shall seek the advice and recommendations of COAC on any proposed Department policies, initiatives, actions, or organizational reforms that will have a major impact on trade and customs revenue functions not later than 45 days prior to the finalization of the policies, initiatives, actions, or organizational reforms.

(2) EXCEPTION.—If the Secretary determines that it is important to the national security interest of the United States to finalize any proposed Department policies, initiatives, actions, or organizational reforms prior to the provision of advice and recommendations described in paragraph (1), the Secretary shall—

(A) seek the advice and recommendations of COAC on the policies, initiatives, actions, or organizational reforms not later than 30 days after the date on which the policies, initiatives, actions, or organizational reforms are finalized; and

(B) to the extent appropriate, modify the policies, initiatives, actions, or organizational reforms based upon the advice and recommendations of COAC.

(c) CONGRESSIONAL CONSULTATION AND NOTIFICATION.—

(1) IN GENERAL.—Subject to paragraph (2), the Secretary shall consult with and provide any recommendations of COAC received under subsection (b) to the appropriate congressional committees not later than 30 days prior to the finalization of any Department policies, initiatives, actions or organizational reforms that will have a major impact on trade and customs revenue functions.

(2) EXCEPTION.—If the Secretary determines that it is important to the national security interest of the United States to finalize any Department policies, initiatives, actions, or organizational reforms prior to the consultation described in paragraph (1), the Secretary shall—

(A) consult with and provide any recommendations of COAC received under subsection (b) to the appropriate congressional committees not later than 30 days after the date on which the policies, initiative, actions, or organizational reforms are finalized; and

(B) to the extent appropriate, modify the policies, initiatives, actions, or organizational reforms based upon the consultations with the appropriate congressional committees.

TITLE VII—MANAGEMENT

SEC. 701. [UNDER SECRETARY FOR MANAGEMENT] *DEPUTY SECRETARY.*

(a) IN GENERAL.—The Secretary, acting through the [Under Secretary for Management] *Deputy Secretary*, shall be responsible for the management and administration of the Department, including the following:

(1) * * *

* * * * * * *

(b) IMMIGRATION.—

(1) IN GENERAL.—In addition to the responsibilities described in subsection (a), the [Under Secretary for Management] *Deputy Secretary* shall be responsible for the following:

(A) * * *

* * * * * * *

(2) TRANSFER OF FUNCTIONS.—In accordance with title XV, there shall be transferred to the [Under Secretary for Management] *Deputy Secretary* all functions performed immediately before such transfer occurs by the Statistics Branch of the Office of Policy and Planning of the Immigration and Naturalization Service with respect to the following programs:

(A) * * *

* * * * * * *

SEC. 702. CHIEF FINANCIAL OFFICER.

(a) In General.—The Chief Financial Officer shall perform functions as specified in chapter 9 of title 31, United States Code, and, with respect to all such functions and other responsibilities that may be assigned to the Chief Financial Officer from time to time,

shall also report to the [Under Secretary for Management] *Deputy Secretary*.

* * * * * * *

(d) AUTHORIZATION LIAISON OFFICER.—

(1) IN GENERAL.—The Chief Financial Officer shall establish the position of Authorization Liaison Officer to provide timely budget and other financial information to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate. The Authorization Liaison Officer shall report directly to the Chief Financial Officer.

(2) SUBMISSION OF REPORTS TO CONGRESS.—The Authorization Liaison Officer shall coordinate with the Appropriations Liaison Officer within the Office of the Chief Financial Officer to ensure, to the greatest extent possible, that all reports prepared for the Committees on Appropriations of the House of Representatives and the Senate are submitted concurrently to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

* * * * * * *

SEC. 705. ESTABLISHMENT OF OFFICER FOR CIVIL RIGHTS AND CIVIL LIBERTIES.

(a) IN GENERAL.—The Officer for Civil Rights and Civil Liberties, who shall report directly to the Secretary, shall—

(1) * * *

* * * * * * *

(5) coordinate with the Privacy Officer to ensure that—

(A) * * *

(B) Congress receives appropriate reports regarding such programs, policies, and procedures; [and]

(6) investigate complaints and information indicating possible abuses of civil rights or civil liberties, unless the Inspector General of the Department determines that any such complaint or information should be investigated by the Inspector General[.]*; and*

(7) serve as the Secretary's coordinator for issues relating to individuals with disabilities and mitigation, preparedness, response, and recovery, by assisting the Secretary and directorates and offices of the Department to develop, implement, and periodically review relevant policies and procedures.

* * * * * * *

SEC. 707. CHIEF SECURITY OFFICER.

(a) ESTABLISHMENT.—There is in the Department a Chief Security Officer.

(b) RESPONSIBILITIES.—The Chief Security Officer shall—

(1) have responsibility for personnel security, facility access, security awareness, and related training;

(2) ensure that each component of the Department complies with Federal standards for security clearances and background investigations;

(3) ensure, to the greatest extent practicable, that individuals in state and local government agencies and private sector entities with a need to receive classified information, receive the appropriate clearances in a timely fashion; and

(4) perform all other functions as determined by the Secretary.

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

Subtitle A—Coordination with Non-Federal Entities

* * * * * * *

SEC. 802. RAIL AND PUBLIC TRANSPORTATION SECURITY TRAINING PROGRAM.

(a) IN GENERAL.—The Secretary, acting through the appropriate Department official with primary responsibility for training programs, and in coordination with the Transportation Security Administration, shall develop and issue detailed guidance for a rail and public transportation worker security training program for the purpose of enhancing the capabilities of rail and public transportation workers, including front-line transit employees such as bus and rail operators, mechanics, customer service employees, maintenance employees, transit police, emergency response providers, and security personnel, to prevent, prepare for, respond to, mitigate against, and recover from threatened or actual acts of terrorism.

(b) PROGRAM ELEMENTS.—The guidance developed under subsection (a) shall provide a program that—

(1) includes, at a minimum, elements that address—

(A) determination of the seriousness of any occurrence;

(B) crew and passenger communication and coordination;

(C) recognition of suspicious behavior or actions and appropriate response;

(D) use of protective devices;

(E) evacuation procedures (including passengers, workers, and those with disabilities);

(F) training exercises regarding various threat conditions, including tunnel evacuation procedures; and

(G) any other subject the Secretary considers appropriate;

(2) is consistent with, and supports implementation of, the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goals, and other national initiatives;

(3) considers existing training programs including Federal or industry programs; and

(4) is evaluated against clear and consistent performance measures.

(c) NATIONAL VOLUNTARY CONSENSUS STANDARDS.—The Secretary shall—

(1) support the development, promulgation, and regular updating as necessary of national voluntary consensus standards for rail and public transportation security training; and

(2) ensure that the training provided under this section is consistent with such standards.

(d) TRAINING PARTNERS.—In developing and delivering training under the program under this section, the Secretary shall—

(1) work with government training facilities, academic institutions, industry and private organizations, employee organizations, and other relevant entities that provide specialized, state-of-the-art training; and

(2) utilize, as appropriate, training provided by industry, public safety academies, State and private colleges and universities, and other facilities.

(e) UPDATES.—The Secretary shall regularly update the training guidance issued under subsection (a) to reflect new or different security threats.

SEC. 803. RAIL AND PUBLIC TRANSPORTATION SECURITY EXERCISE PROGRAM.

(a) IN GENERAL.—The Secretary, acting through the Department official with primary responsibility for grants and training, shall establish a Rail and Public Transportation Security Exercise Program (hereinafter in this section referred to as the "Program") for the purpose of testing and evaluating the capabilities of Federal, State, and local agencies and tribal governments, rail and public transportation system employees and management, governmental and nongovernmental emergency response providers, the private sector, or any other organization or entity, as the Secretary determines to be appropriate, to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism, natural disasters, and other emergencies at rail and public transportation systems.

(b) REQUIREMENTS.—The Secretary, acting through the Department official with primary responsibility for grants and training, and in coordination with the Assistant Secretary of Homeland Security (Transportation Security Administration), shall ensure that the Program—

(1) consolidates all existing rail and public transportation system security exercise programs administered by the Department;

(2) conducts, on a periodic basis, exercises at rail and public transportation systems that are—

(A) scaled and tailored to the needs of each rail and public transportation system;

(B) live in the case of the most at-risk rail and public transportation systems;

(C) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(D) consistent with the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goal, and other such national initiatives;

(E) evaluated against clear and consistent performance measures;

(F) assessed to learn best practices, which shall be shared with appropriate Federal, State, local and tribal officials, rail and public transportation system employees and management; governmental and nongovernmental emergency response providers, and the private sector; and

(G) followed by remedial action in response to lessons learned; and

(3) assists State and local governments and rail and public transportation systems in designing, implementing, and evaluating exercises that—

(A) conform to the requirements of paragraph (2); and

(B) are consistent with any applicable State or Urban Area Homeland Security Plan.

(c) REMEDIAL ACTION MANAGEMENT SYSTEM.—The Secretary, acting through the Department official with primary responsibility for grants and training, shall establish a Remedial Action Management System to—

(1) identify and analyze each rail and public transportation system exercise for lessons learned and best practices;

(2) disseminate lessons learned and best practices to participants in the Program;

(3) monitor the implementation of lessons learned and best practices by participants in the Program; and

(4) conduct remedial action tracking and long-term trend analysis.

(d) GRANT PROGRAM FACTOR.—In evaluating and prioritizing applications for Federal financial assistance under section 513, the Secretary shall give additional consideration to those applicants that have conducted rail and public transportation security exercises under this section.

(e) CONSULTATION.—The Secretary shall ensure that, in carrying out the Program, the Department official with primary responsibility for grants and training shall consult with—

(1) a geographic and substantive cross section of governmental and nongovernmental emergency response providers; and

(2) rail and public transportation system personnel and management.

* * * * * * *

Subtitle H—Miscellaneous Provisions

* * * * * * *

SEC. 875. MISCELLANEOUS AUTHORITIES.

(a) * * *

* * * * * * *

(d) PROTECTION OF NAME, INITIALS, INSIGNIA, AND SEAL.—

(1) IN GENERAL.—Except with the written permission of the Secretary, no person may knowingly use, in connection with any advertisement, commercial activity, audiovisual production (including film or television production), impersonation, Internet

domain name, Internet e-mail address, or Internet web site, merchandise, retail product, or solicitation in a manner reasonably calculated to convey the impression that the Department or any organizational element of the Department has approved, endorsed, or authorized such use, any of the following (or any colorable imitation thereof):

(A) The words "Department of Homeland Security", the initials "DHS", the insignia or seal of the Department, or the title "Secretary of Homeland Security".

(B) The name, initials, insignia, or seal of any organizational element (including any former such element) of the Department, or the title of any other officer or employee of the Department, notice of which has been published by the Secretary of Homeland Security in accordance with paragraph (3).

(2) CIVIL ACTION.—Whenever it appears to the Attorney General that any person is engaged or is about to engage in an act or practice that constitutes or will constitute conduct prohibited by subsection (d)(1), the Attorney General may initiate a civil proceeding in a district court of the United States to enjoin such act or practice. Such court shall proceed as soon as practicable to the hearing and determination of such action and may, at any time before final determination, enter such restraining orders or prohibitions, or take such other actions as is warranted, to prevent injury to the United States or to any person or class of persons for whose protection the action is brought.

(3) NOTICE AND PUBLICATION.—The notice and publication to which paragraph (1)(B) refers is a notice published in the Federal Register including the name, initials, seal, or class of titles protected under paragraph (1)(B) and a statement that they are protected under that provision. The Secretary may amend such notices from time to time as the Secretary determines appropriate in the public interest and shall publish such amendments in the Federal Register.

(4) AUDIOVISUAL PRODUCTION.—For the purpose of this subsection, the term "audiovisual production" means the production of a work that consists of a series of related images that are intrinsically intended to be shown by the use of machines or devices such as projectors, viewers, or electronic equipment, together with accompanying sounds, if any, regardless of the nature of the material objects, such as films or tapes, in which the work is embodied.

* * * * * * *

[SEC. 879. OFFICE OF INTERNATIONAL AFFAIRS.

[(a) ESTABLISHMENT.—There is established within the Office of the Secretary an Office of International Affairs. The Office shall be headed by a Director, who shall be a senior official appointed by the Secretary.

[(b) DUTIES OF THE DIRECTOR.—The Director shall have the following duties:

[(1) To promote information and education exchange with nations friendly to the United States in order to promote sharing of best practices and technologies relating to homeland security. Such exchange shall include the following:

[(A) Exchange of information on research and development on homeland security technologies.

[(B) Joint training exercises of first responders.

[(C) Exchange of expertise on terrorism prevention, response, and crisis management.

[(2) To identify areas for homeland security information and training exchange where the United States has a demonstrated weakness and another friendly nation or nations have a demonstrated expertise.

[(3) To plan and undertake international conferences, exchange programs, and training activities.

[(4) To manage international activities within the Department in coordination with other Federal officials with responsibility for counter-terrorism matters.]

* * * * * * *

SEC. 888. PRESERVING COAST GUARD MISSION PERFORMANCE.

(a) * * *

* * * * * * *

(f) ANNUAL REVIEW.—

(1) * * *

(2) REPORT.—The report under this paragraph shall be submitted to—

[(A) the Committee on Governmental Affairs of the Senate;]

(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

(B) the Committee on Homeland Security of the House of Representatives;

[(B)] *(C)* the Committee on Government Reform of the House of Representatives;

[(C)] *(D)* the Committees on Appropriations of the Senate and the House of Representatives;

[(D)] *(E)* the Committee on Commerce, Science, and Transportation of the Senate; and

[(E)] *(F)* the Committee on Transportation and Infrastructure of the House of Representatives.

* * * * * * *

SEC. 890A. HOMELAND SECURITY PROCUREMENT TRAINING.

(a) ESTABLISHMENT.—The Chief Procurement Officer shall provide homeland security procurement training to acquisition employees.

(b) RESPONSIBILITIES OF CHIEF PROCUREMENT OFFICER.—The Chief Procurement Officer shall carry out the following responsibilities:

(1) Establish objectives to achieve the efficient and effective use of available acquisition resources by coordinating the acquisition education and training programs of the Department and tailoring them to support the careers of acquisition employees.

(2) Develop, in consultation with the Council on Procurement Training established under subsection (d), the curriculum of the homeland security procurement training to be provided.

(3) Establish, in consultation with the Council on Procurement Training, training standards, requirements, and courses to be required for acquisition employees.

(4) Establish an appropriate centralized mechanism to control the allocation of resources for conducting such required courses and other training and education.

(5) Select course providers and certify courses to ensure that the procurement training curriculum supports a coherent framework for the educational development of acquisition employees, including the provision of basic, intermediate, and advanced courses.

(6) Publish an annual catalog that includes a list of the acquisition education and training courses.

(7) Develop a system of maintaining records of student enrollment, and other data related to students and courses conducted pursuant to this section.

(c) PROVISION OF INSTRUCTION.—The Chief Procurement Officer shall provide procurement training to acquisition employees of any office under subsection (d)(3). The appropriate member of the Council on Procurement Training may direct such an employee to receive procurement training.

(d) COUNCIL ON PROCUREMENT TRAINING.—

(1) ESTABLISHMENT.—The Secretary shall establish a Council on Procurement Training to advise and make policy and curriculum recommendations to the Chief Procurement Officer.

(2) CHAIR OF COUNCIL.—The chair of the Council on Procurement Training shall be the Deputy Chief Procurement Officer.

(3) MEMBERS.—The members of the Council on Procurement Training are the chief procurement officers of each of the following:

(A) United States Customs and Border Protection.

(B) The Transportation Security Administration.

(C) The Office of Procurement Operations.

(D) The Bureau of Immigration and Customs Enforcement.

(E) The Federal Emergency Management Agency.

(F) The Coast Guard.

(G) The Federal Law Enforcement Training Center.

(H) The United States Secret Service.

(I) Such other entity as the Secretary determines is appropriate.

(e) ACQUISITION EMPLOYEE DEFINED.—For purposes of this section, the term "acquisition employee" means an employee serving under a career or career-conditional appointment in the competitive service or appointment of equivalent tenure in the excepted service of the Federal Government, at least 50 percent of whose assigned duties include acquisitions, procurement-related program management, or procurement-related oversight functions.

(f) REPORT REQUIRED.—Not later than March 1 of each year, the Chief Procurement Officer shall submit to the Secretary a report on the procurement training provided under this section, which shall include information about student enrollment, students who enroll but do not attend courses, graduates, certifications, and other relevant information.

* * * * * * *

TITLE XVIII—MISCELLANEOUS PROVISIONS

Subtitle A—Canine Detection Teams

SEC. 1801. COORDINATION AND ENHANCEMENT OF CANINE DETECTION TEAM TRAINING.

The Secretary shall—

(1) fully coordinate the canine training programs of the Department that support the Department's counter-terrorism, counter-smuggling, transportation security, and border security missions and other missions of the Department, including, with respect to the research and development of new canine training methods, the optimum number and type of training aids, and measurements for efficiency and effectiveness;

(2) ensure that the Department is maximizing its use of existing training facilities and resources to train canines throughout the year; and

(3) coordinate the use of detection canines trained by other Federal agencies, nonprofit organizations, universities, and private training facilities in order to increase the number of trained detection canines available to Federal, State, and local law enforcement agencies.

SEC. 1802. CANINE PROCUREMENT.

The Secretary shall—

(1) make it a priority to increase the number of domestically bred canines used by the Department to assist in its counter-terrorism mission, including the protection of ports of entry and along the United States border;

(2) increase the utilization of domestically bred canines from universities and private and nonprofit sources in the United States; and

(3) consult with other Federal, State, and local agencies, nonprofit organizations, universities, and private entities that use detection canines, such as those participating in the Scientific Working Group on Dog and Orthogonal Detectors (popularly known as "SWGDOG"), as well as the Office of Management and Budget, to encourage domestic breeding of canines and consolidate canine procurement, where possible, across the Federal Government to reduce the cost of purchasing canines.

SEC. 1803. DOMESTIC CANINE BREEDING GRANT PROGRAM.

(a) ESTABLISHMENT OF PROGRAM.—The Secretary shall establish a competitive grant program for domestic breeders of canines. The purpose of the grant program shall be to encourage the development and growth of canine breeds that are best suited for detection training purposes within the United States and to encourage the development of applied research into enhancement of working dog performance and health traits.

(b) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $3,000,000 for each of fiscal years 2007 through 2011.

SEC. 1804. HOMELAND SECURITY CANINE DETECTION ACCREDITATION BOARD.

(a) ESTABLISHMENT OF ACCREDITATION BOARD.—

(1) IN GENERAL.—Not later than 180 days after the date on which the national voluntary consensus standards referred to in subsection (b)(1) are issued, the Secretary, in consultation with the Secretary of Defense, the Secretary of State, and the Attorney General, shall establish a Homeland Security Canine Detection Accreditation Board to develop and implement a process for certifying compliance with such standards.

(2) MEMBERSHIP.—The membership of the Accreditation Board shall consist of experts in the fields of canine training and explosives detection from Federal and State agencies, universities, other research institutions, and the private sector, such as those represented on the Executive Board of SWGDOG.

(b) ACCREDITATION PROCESS.—The Accreditation Board shall establish and implement a voluntary accreditation process to—

(1) certify that persons conducting certification of canine detection teams appropriately ensure that the canine detection teams meet the national voluntary consensus standards developed by SWGDOG;

(2) ensure that canine detection teams do not put public safety and the safety of law enforcement personnel at risk due to fraud or weaknesses in the initial or maintenance training curriculum; and

(3) maintain and update a public list of entities accredited by the Department to certify canine detection teams.

(c) COMPLIANCE WITH STANDARDS.—Beginning not later than the date that is 180 days after the date on which the standards referred to in subsection (b)(1) are issued, the Secretary shall require that grant funds administered by the Department may not be used to acquire a canine detection team unless—

(1) the canine detection team is certified under the process established under subsection (b); or

(2) the Secretary determines that the applicant has shown special circumstances that justify the acquisition of canines that are not certified under the process established under subsection (b).

SEC. 1805. DEFINITIONS.

In this subtitle:

(1) CANINE DETECTION TEAM.—The term "canine detection team" means a canine and a canine handler.

(2) CERTIFYING ENTITY.—The term "certifying entity" means an entity that oversees the processes and procedures used to train and test canine detection teams.

(3) SWGDOG.—The term "SWGDOG" means the Scientific Working Group of Dog and Orthogonal Detectors.

[TITLE VI—TREATMENT OF CHARITABLE TRUSTS FOR MEMBERS OF THE ARMED FORCES OF THE UNITED STATES AND OTHER GOVERNMENTAL ORGANIZATIONS]

Subtitle B—Treatment of Certain Charitable Trusts

SEC. [601] *1811*. TREATMENT OF CHARITABLE TRUSTS FOR MEMBERS OF THE ARMED FORCES OF THE UNITED STATES AND OTHER GOVERNMENTAL ORGANIZATIONS.

(a) FINDINGS.—Congress finds the following:

(1) * * *

* * * * * * *

TITLE XIX—DOMESTIC NUCLEAR DETECTION

SEC. 1901. OFFICE OF DOMESTIC NUCLEAR DETECTION.

(a) IN GENERAL.—There shall be in the Department of Homeland Security an Office of Domestic Nuclear Detection.

(b) PURPOSE.—The purpose of the Office shall be to protect against the unauthorized importation, possession, storage, transportation, development, or use of a nuclear explosive device, fissile material, or radiological material against the United States.

(c) DIRECTOR.—The Office shall be headed by a Director of Domestic Nuclear Detection, who shall be appointed by the President from among individuals nominated by the Secretary. No individual shall be appointed Director of Domestic Nuclear Detection unless the individual has by education or experience demonstrated knowledge, ability, and skill in a field applicable to the detection and prevention of nuclear or radiological terrorism.

(d) LIMITATION.—This title shall not be construed to affect the performance, by directorates and agencies of the Department other than the Office, of functions that are not related to detection and prevention of nuclear and radiological terrorism.

SEC. 1902. RESPONSIBILITIES OF DIRECTOR OF DOMESTIC NUCLEAR DETECTION.

(a) IN GENERAL.—The Secretary shall vest in the Director of Domestic Nuclear Detection the primary responsibility in the Department for—

(1) administering all nuclear and radiological detection and prevention functions and assets of the Department; and

(2) for coordinating such administration with nuclear and radiological detection and prevention activities of other Federal departments and agencies.

(b) TRANSFER OF FUNCTIONS.—The Secretary shall transfer to the Director the authority to administer, or supervise the administration of, all functions, personnel, assets, and liabilities of all Department

programs and projects relating to nuclear and radiological detection research, development, testing, and evaluation, and nuclear and radiological detection system acquisition and deployment, including with respect to functions and assets transferred by section 303(1)(B), (C), and (E) and functions, assets, and personnel transferred pursuant to section 1910(c).

SEC. 1903. GLOBAL NUCLEAR DETECTION ARCHITECTURE.

(a) IN GENERAL.—The Director of Domestic Nuclear Detection shall coordinate the Federal Government's implementation of a global nuclear detection architecture.

(b) FUNCTIONS OF DIRECTOR.—In carrying out subsection (a), the Director shall—

(1) design a strategy that will guide deployment of the global nuclear detection architecture;

(2) implement the strategy in the United States; and

(3) coordinate Department and Federal interagency efforts to deploy the elements of the global nuclear detection architecture outside the United States.

(c) RELATIONSHIP TO OTHER DEPARTMENTS AND AGENCIES.—The authority of the Director under this section shall not affect an authority or responsibility of any other department or agency of the Federal Government with respect to the deployment of nuclear and radiological detection systems outside the United States under any program administered by that department or agency.

SEC. 1904. RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—The Director of Domestic Nuclear Detection shall carry out a research and development program to achieve transformational and evolutionary improvements in detection capabilities for shielded and unshielded nuclear explosive devices and radiological dispersion devices.

(b) HIGH-RISK PROJECTS.—The program shall include funding for transformational research and development projects that may have a high risk of failure but have the potential to provide significant benefits.

(c) LONG-TERM PROJECTS.—In order to reflect a long-term commitment to the development of more effective detection technologies, the program shall include the provision of funding for projects having a duration of more than 3 years, as appropriate.

(d) COORDINATION WITH OTHER FEDERAL PROGRAMS.—The Director shall coordinate implementation of the program with other Federal agencies performing similar research and development in order to accelerate the development of effective technologies, promote technology sharing, and to avoid duplication, including through the use of the interagency coordination council established under section 1913.

SEC. 1905. SYSTEM ASSESSMENTS.

(a) PROGRAM REQUIRED.—The Director of Domestic Nuclear Detection shall carry out a program to test and evaluate technology for detecting nuclear explosive devices and fissile or radiological material.

(b) PERFORMANCE METRICS.—The Director shall establish performance metrics for evaluating the effectiveness of individual detectors and detection systems in detecting nuclear explosive devices or fissile or radiological material—

(1) under realistic operational and environmental conditions; and

(2) against realistic adversary tactics and countermeasures.

(c) PROVISION OF TESTING SERVICES.—

(1) IN GENERAL.—The Director may, under the program required under subsection (a), make available testing services to developers of detection technologies. The results of the tests performed with services made available under this subsection shall be confidential and may not be disclosed to individuals or entities outside of the Federal Government without the consent of the developer for whom the tests are performed.

(2) FEES.—The Director may charge a fee, as appropriate, to perform any service under this subsection.

(d) SYSTEM ASSESSMENTS.—

(1) IN GENERAL.—The Director shall periodically perform system-wide assessments of the global nuclear detection architecture to identify vulnerabilities and to gauge overall system performance against nuclear and radiological threats.

(2) INCLUDED ACTIVITIES.—The assessments shall include—

(A) red teaming activities to identify vulnerabilities and possible modes of attack and concealment methods; and

(B) net assessments to determine architecture performance against adversary tactics and concealment methods.

(3) USE.—The Director shall use the assessments to guide deployment of the global nuclear detection architecture and the research and development activities of the Office of Domestic Nuclear Detection.

SEC. 1906. TECHNOLOGY ACQUISITION, DEPLOYMENT, SUPPORT, AND TRAINING.

(a) ACQUISITION STRATEGY.—

(1) IN GENERAL.—The Director of Domestic Nuclear Detection shall develop and, subject to the availability of appropriations, execute a strategy for the acquisition and deployment of detection systems in order to implement the Department components of the global nuclear detection architecture developed under section 1903.

(2) USE OF AVAILABLE CONTRACTING PROCEDURES.—The Director shall make use of all contracting procedures available to the Secretary to implement the acquisition strategy.

(3) DETERMINATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGY.—The Director shall make recommendations based on the criteria included in section 862(b) as to whether the detection systems acquired pursuant to this subsection shall be designated by the Secretary as anti-terrorism technologies that qualify for protection under the system of risk management under subtitle G of title VIII. The Under Secretary for Science and Technology shall consider the Director's recommendations and expedite the process of determining whether such detection systems shall be designated as anti-terrorism technologies that qualify for such protection.

(b) DEPLOYMENT.—The Director shall deploy detection systems for use by Department operational units and other end-users in implementing the global nuclear detection architecture.

(c) OPERATIONAL SUPPORT AND PROTOCOLS.—

(1) OPERATIONAL SUPPORT.—The Director shall provide operational support for all systems acquired to implement the acquisition strategy developed under subsection (a).

(2) OPERATIONAL PROTOCOLS.—The Director shall develop operational protocols for detection technology acquired and deployed to implement the acquisition strategy, including procedures for alarm resolution and notification of appropriate response agencies in the event that illicit nuclear, radioactive, or fissile materials are detected by such a product or service.

(3) TECHNICAL REACHBACK.—The Director will ensure that the expertise necessary to accurately interpret detection data is made available in a timely manner for all technology deployed to implement the global nuclear detection architecture.

(d) TRAINING.—The Director shall develop and distribute training materials and provide training to all end-users of technology acquired by the Director under the acquisition strategy.

(e) SOLICITATION OF END-USER INPUT.—In developing requirements for the research and development program of section 1904 and requirements for the acquisition of detection systems to implement the strategy in subsection (a), the Director shall solicit input from end-users of such systems.

(f) STATE AND LOCAL SUPPORT.—Upon request, the Director shall provide guidance regarding radiation detection technology acquisitions to be made by State, local, and tribal governments and emergency response providers.

SEC. 1907. SITUATIONAL AWARENESS.

(a) DETECTION INFORMATION.—The Director of Domestic Nuclear Detection—

(1) shall continuously monitor detection information received from foreign and domestic detection systems to maintain for the Department a situational awareness of all nuclear threats; and

(2) shall gather and archive—

(A) detection data measurements taken of benign activities in the normal flows of commerce; and

(B) alarm data, including false alarms and nuisance alarms.

(b) INFORMATION SHARING.—The Director shall coordinate with other governmental agencies to ensure that the detection of unauthorized nuclear explosive devices, fissile material, or radiological material is promptly reported to all appropriate Federal response agencies including the Attorney General, the Director of the Federal Bureau of Investigation, the Secretary of Defense, and the Secretary of Energy.

(c) INCIDENT RESOLUTION.—The Director shall assess nuclear threats communicated by Federal, State, tribal, or local officials and provide adequate technical reachback capability for swift and effective incident resolution.

(d) SECURITY.—The Director shall—

(1) develop and implement security standards and protocols for the control and protection of all classified or sensitive information in possession of the Office; and

(2) ensure that relevant personnel of the Office have the required security clearances to properly handle such information.

SEC. 1908. FORENSIC ANALYSIS.

The Director of Domestic Nuclear Detection shall perform all research, development, and acquisition activities of the Department pertaining to forensic analysis and attribution of nuclear and radiological attacks.

SEC. 1909. THREAT INFORMATION.

(a) THREAT ASSESSMENTS.—The Director of Domestic Nuclear Detection shall utilize classified and unclassified nuclear and radiological threat assessments in designing the global nuclear detection architecture under section 1903, prioritizing detection system deployments, and testing and optimizing system performance of that architecture, including assessments of—

(1) smuggling routes;

(2) locations of relevant nuclear and radiological material throughout the world;

(3) relevant terrorist tradecraft and concealment methods; and

(4) relevant nuclear and radiological threat objects in terms of possible detection signatures.

(b) ACCESS TO INFORMATION.—The Secretary shall provide the Director access to all information relating to nuclear and radiological threats, including reports, assessments, analyses, and unevaluated intelligence, that is necessary to successfully design, deploy, and support the operation of an effective global detection architecture under section 1903.

(c) ANALYTICAL SUPPORT.—The Director shall request that the Secretary provide to the Director, pursuant to section 201(c)(20), the requisite intelligence and information analysis support necessary to effectively discharge the Director's responsibilities.

(d) ANALYTICAL EXPERTISE.—For the purposes of performing any of the assessments required under subsection (a), the Director, subject to the availability of appropriations, may hire qualified personnel with experience in performing nuclear and radiological threat assessments.

(e) COLLECTION REQUESTS.—The Director shall recommend that the Secretary consult with the Director of Central Intelligence or other appropriate intelligence, law enforcement, or other elements of the Federal Government pursuant to section 201(c)(7) with respect to intelligence collection to design, deploy, and support the operation of the global detection architecture under section 1903.

SEC. 1910. ADMINISTRATIVE AUTHORITIES.

(a) HIRING.—In hiring personnel for the Office of Domestic Nuclear Detection, the Secretary shall have the hiring and management authorities described in section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note; Public Law 105-261). The term of appointments for employees under subsection (c)(1) of that section may not exceed 5 years before the granting of any extension under subsection (c)(2) of that section

(b) DETAIL OF PERSONNEL.—In order to assist the Director of Domestic Nuclear Detection in discharging the Director's responsibilities, personnel of other Federal agencies may be detailed to the Office for the performance of analytic functions and related duties.

(c) TRANSFER OF SCIENCE AND TECHNOLOGY FUNCTIONS, PERSONNEL, AND ASSETS.—

(1) TRANSFER REQUIRED.—Except as provided in paragraph (2), the Secretary shall transfer to the Director the functions, assets, and personnel of the Department relating to radiological and nuclear countermeasures, including forensics of contaminated evidence and attack attribution.

(2) EXCEPTIONS.—The Secretary shall not transfer under paragraph (1) functions, assets, and personnel relating to consequence management and recovery.

(3) ELIMINATION OF DUPLICATION OF EFFORT.—The Secretary shall ensure that to the extent that complementary functions are vested in the Directorate of Science and Technology and the Office of Domestic Nuclear Detection with respect to radiological and nuclear countermeasures, the Under Secretary for Science and Technology and the Director of Domestic Nuclear Detection coordinate the programs administered by the Under Secretary and the Director to eliminate duplication and increase integration opportunities, particularly with respect to technology development and test and evaluation.

SEC. 1911. REPORT REQUIREMENT.

The Director of Domestic Nuclear Detection shall submit to Congress an annual report on each of the following:

(1) The global detection strategy developed under section 1903.

(2) The status of implementation of such architecture.

(3) The schedule for future detection system deployments under such architecture.

(4) The research and development program of the Office of Domestic Nuclear Detection.

(5) A summary of actions taken by the Office during the reporting period to counter nuclear and radiological threats.

SEC. 1912. ADVISORY COUNCIL ON NUCLEAR DETECTION.

(a) ESTABLISHMENT.—Pursuant to section 871 of this Act, the Secretary shall establish within the Office of Domestic Nuclear Detection an Advisory Council on Nuclear Detection (in this section referred to as the "Advisory Council"). The Advisory Council shall report to the Director of Domestic Nuclear Detection.

(b) FUNCTIONS.—The Advisory Council shall, at the request of the Director—

(1) advise the Director on recommendations for the global nuclear detection architecture developed under section 1903(a);

(2) identify research areas for development of next-generation and transformational nuclear and radiological detection technologies; and

(3) and have such additional responsibilities as the Director may assign in furtherance of the Department's homeland security mission with respect to enhancing domestic and international nuclear and radiological detection capabilities.

(c) MEMBERSHIP.—The Advisory Council shall consist of 5 members appointed by the Director, who shall—

(1) be individuals who have an eminent knowledge and technical expertise related to nuclear and radiological detection research and development and radiation detection;

(2) be selected solely on the basis of their established record of distinguished service; and

(3) not be employees of the Federal Government, other than employees of National Laboratories.

(d) CONFLICT OF INTEREST RULES.—The Advisory Council shall establish rules for determining when one of its members has a conflict of interest in a matter being considered by the Advisory Council, and the appropriate course of action to address such conflicts of interest.

SEC. 1913. INTERAGENCY COORDINATION COUNCIL.

The President—

(1) shall establish an interagency coordination council to facilitate interagency cooperation for purposes of implementing this title;

(2) shall appoint the Secretary to chair the interagency coordination council; and

(3) may appoint the Attorney General, the Secretary of Energy, the Secretary of State, the Secretary of Defense, and the heads of other appropriate Federal agencies to designate members to serve on such council.

SEC. 1914. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated to carry out this title—

(1) from the amount authorized to be appropriated for fiscal year 2007 under section 101 of the Department of Homeland Security Authorization Act for Fiscal Year 2007, $536,000,000 for that fiscal year; and

(2) such sums as may be necessary for each subsequent fiscal year.

SEC. 1915. DEFINITIONS.

In this title:

(1) The term "fissile materials" means material capable of undergoing nuclear fission by thermal or slow neutrons.

(2) The term "global nuclear detection architecture" means a multi-layered system of detectors deployed internationally and domestically to detect and interdict nuclear and radiological materials intended for illicit use.

(3) The term "nuclear and radiological detection system" means any technology that is capable of detecting or identifying nuclear and radiological material or explosive devices.

(4) The term "radiological material" means material that emits nuclear radiation.

(5) The term "nuclear explosive device" means an explosive device capable of producing a nuclear yield.

(6) The term "technical reachback" means technical expert support provided to operational end users for data interpretation and alarm resolution.

(7) The term "transformational" means that, if successful, will produce dramatic technological improvements over existing capabilities in the areas of performance, cost, or ease of use.

TITLE XX—FUNDING FOR FIRST RESPONDERS

SEC. 2001. DEFINITIONS.

In this title:

(1) BOARD.—The term "Board" means the First Responder Grants Board established under section 2004.

(2) COVERED GRANT.—The term "covered grant" means any grant to which this title applies under section 2002.

(3) DIRECTLY ELIGIBLE TRIBE.—The term "directly eligible tribe" means any Indian tribe or consortium of Indian tribes that—

(A) meets the criteria for inclusion in the qualified applicant pool for Self-Governance that are set forth in section 402(c) of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 458bb(c));

(B) employs at least 10 full-time personnel in a law enforcement or emergency response agency with the capacity to respond to calls for law enforcement or emergency services; and

(C)(i) is located on, or within 5 miles of, an international border or waterway;

(ii) is located within 5 miles of a facility designated as high-risk critical infrastructure by the Secretary;

(iii) is located within or contiguous to one of the 50 largest metropolitan statistical areas in the United States; or

(iv) has more than 1,000 square miles of Indian country, as that term is defined in section 1151 of title 18, United States Code.

(4) ELEVATIONS IN THE THREAT ALERT LEVEL.—The term "elevations in the threat alert level" means any designation (including those that are less than national in scope) that raises the homeland security threat level to either the highest or second highest threat level under the Homeland Security Advisory System referred to in section 201(d)(7).

(5) EMERGENCY PREPAREDNESS.—The term "emergency preparedness" shall have the same meaning that term has under section 602 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5195a).

(6) ESSENTIAL CAPABILITIES.—The term "essential capabilities" means the levels, availability, and competence of emergency personnel, planning, training, and equipment across a variety of disciplines needed to effectively and efficiently prevent, prepare for, respond to, and recover from acts of terrorism consistent with established practices.

(7) FIRST RESPONDER.—The term "first responder" shall have the same meaning as the term "emergency response provider".

(8) INDIAN TRIBE.—The term "Indian tribe" means any Indian tribe, band, nation, or other organized group or community, including any Alaskan Native village or regional or village corporation as defined in or established pursuant to the Alaskan Native Claims Settlement Act (43 U.S.C. 1601 et seq.), which is recognized as eligible for the special programs and services pro-

vided by the United States to Indians because of their status as Indians.

(9) REGION.—The term "region" means—

(A) any geographic area consisting of all or parts of 2 or more contiguous States, counties, municipalities, or other local governments that have a combined population of at least 1,650,000 or have an area of not less than 20,000 square miles, and that, for purposes of an application for a covered grant, is represented by 1 or more governments or governmental agencies within such geographic area, and that is established by law or by agreement of 2 or more such governments or governmental agencies in a mutual aid agreement; or

(B) any other combination of contiguous local government units (including such a combination established by law or agreement of two or more governments or governmental agencies in a mutual aid agreement) that is formally certified by the Secretary as a region for purposes of this Act with the consent of—

(i) the State or States in which they are located, including a multi-State entity established by a compact between two or more States; and

(ii) the incorporated municipalities, counties, and parishes that they encompass.

(10) TERRORISM PREPAREDNESS.—The term "terrorism preparedness" means any activity designed to improve the ability to prevent, prepare for, respond to, mitigate against, or recover from threatened or actual terrorist attacks.

SEC. 2002. FASTER AND SMARTER FUNDING FOR FIRST RESPONDERS.

(a) COVERED GRANTS.—This title applies to grants provided by the Department to States, regions, or directly eligible tribes for the primary purpose of improving the ability of first responders to prevent, prepare for, respond to, mitigate against, or recover from threatened or actual terrorist attacks, especially those involving weapons of mass destruction, administered under the following:

(1) STATE HOMELAND SECURITY GRANT PROGRAM.—The State Homeland Security Grant Program of the Department, or any successor to such grant program.

(2) URBAN AREA SECURITY INITIATIVE.—The Urban Area Security Initiative of the Department, or any successor to such grant program.

(3) LAW ENFORCEMENT TERRORISM PREVENTION PROGRAM.—The Law Enforcement Terrorism Prevention Program of the Department, or any successor to such grant program.

(b) EXCLUDED PROGRAMS.—This title does not apply to or otherwise affect the following Federal grant programs or any grant under such a program:

(1) NONDEPARTMENT PROGRAMS.—Any Federal grant program that is not administered by the Department.

(2) FIRE GRANT PROGRAMS.—The fire grant programs authorized by sections 33 and 34 of the Federal Fire Prevention and Control Act of 1974 (15 U.S.C. 2229, 2229a).

(3) EMERGENCY MANAGEMENT PLANNING AND ASSISTANCE ACCOUNT GRANTS.—The Emergency Management Performance Grant program and the Urban Search and Rescue Grants pro-

gram authorized by title VI of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5195 et seq.); the Departments of Veterans Affairs and Housing and Urban Development, and Independent Agencies Appropriations Act, 2000 (113 Stat. 1047 et seq.); and the Earthquake Hazards Reduction Act of 1977 (42 U.S.C. 7701 et seq.).

SEC. 2003. COVERED GRANT ELIGIBILITY AND CRITERIA.

(a) GRANT ELIGIBILITY.—Any State, region, or directly eligible tribe shall be eligible to apply for a covered grant.

(b) GRANT CRITERIA.—The Secretary shall award covered grants to assist States and local governments in achieving, maintaining, and enhancing the essential capabilities for terrorism preparedness established by the Secretary.

(c) STATE HOMELAND SECURITY PLANS.—

(1) SUBMISSION OF PLANS.—The Secretary shall require that any State applying to the Secretary for a covered grant must submit to the Secretary a 3-year State homeland security plan that—

(A) describes the essential capabilities that communities within the State should possess, or to which they should have access, based upon the terrorism risk factors relevant to such communities, in order to meet the Department's goals for terrorism preparedness;

(B) demonstrates the extent to which the State has achieved the essential capabilities that apply to the State;

(C) demonstrates the needs of the State necessary to achieve, maintain, or enhance the essential capabilities that apply to the State;

(D) includes a prioritization of such needs based on threat, vulnerability, and consequence assessment factors applicable to the State;

(E) describes how the State intends—

(i) to address such needs at the city, county, regional, tribal, State, and interstate level, including a precise description of any regional structure the State has established for the purpose of organizing homeland security preparedness activities funded by covered grants;

(ii) to use all Federal, State, and local resources available for the purpose of addressing such needs; and

(iii) to give particular emphasis to regional planning and cooperation, including the activities of multijurisdictional planning agencies governed by local officials, both within its jurisdictional borders and with neighboring States;

(F) with respect to the emergency preparedness of first responders, addresses the unique aspects of terrorism as part of a comprehensive State emergency management plan; and

(G) provides for coordination of response and recovery efforts at the local level, including procedures for effective incident command in conformance with the National Incident Management System.

(2) CONSULTATION.—The State plan submitted under paragraph (1) shall be developed in consultation with and subject to appropriate comment by local governments and first responders within the State.

(3) APPROVAL BY SECRETARY.—The Secretary may not award any covered grant to a State unless the Secretary has approved the applicable State homeland security plan.

(4) REVISIONS.—A State may revise the applicable State homeland security plan approved by the Secretary under this subsection, subject to approval of the revision by the Secretary.

(d) CONSISTENCY WITH STATE PLANS.—The Secretary shall ensure that each covered grant is used to supplement and support, in a consistent and coordinated manner, the applicable State homeland security plan or plans.

(e) APPLICATION FOR GRANT.—

(1) IN GENERAL.—Except as otherwise provided in this subsection, any State, region, or directly eligible tribe may apply for a covered grant by submitting to the Secretary an application at such time, in such manner, and containing such information as is required under this subsection, or as the Secretary may reasonably require.

(2) DEADLINES FOR APPLICATIONS AND AWARDS.—All applications for covered grants must be submitted at such time as the Secretary may reasonably require for the fiscal year for which they are submitted. The Secretary shall award covered grants pursuant to all approved applications for such fiscal year as soon as practicable, but not later than March 1 of such year.

(3) AVAILABILITY OF FUNDS.—All funds awarded by the Secretary under covered grants in a fiscal year shall be available for obligation through the end of the subsequent fiscal year.

(4) MINIMUM CONTENTS OF APPLICATION.—The Secretary shall require that each applicant include in its application, at a minimum—

(A) the purpose for which the applicant seeks covered grant funds and the reasons why the applicant needs the covered grant to meet the essential capabilities for terrorism preparedness within the State, region, or directly eligible tribe to which the application pertains;

(B) a description of how, by reference to the applicable State homeland security plan or plans under subsection (c), the allocation of grant funding proposed in the application, including, where applicable, the amount not passed through to local governments, first responders, and other local groups, would assist in fulfilling the essential capabilities for terrorism preparedness specified in such plan or plans;

(C) a statement of whether a mutual aid agreement applies to the use of all or any portion of the covered grant funds;

(D) if the applicant is a State, a description of how the State plans to allocate the covered grant funds to regions, local governments, and Indian tribes;

(E) if the applicant is a region—

(i) a precise geographical description of the region and a specification of all participating and nonparticipating local governments within the geographical area comprising that region;

(ii) a specification of what governmental entity within the region will administer the expenditure of funds under the covered grant; and

(iii) a designation of a specific individual to serve as regional liaison;

(F) a capital budget showing how the applicant intends to allocate and expend the covered grant funds;

(G) if the applicant is a directly eligible tribe, a designation of a specific individual to serve as the tribal liaison; and

(H) a statement of how the applicant intends to meet the matching requirement, if any, that applies under section 2005(g).

(5) REGIONAL APPLICATIONS.—

(A) RELATIONSHIP TO STATE APPLICATIONS.—A regional application—

(i) shall be coordinated with an application submitted by the State or States of which such region is a part;

(ii) shall supplement and avoid duplication with such State application; and

(iii) shall address the unique regional aspects of such region's terrorism preparedness needs beyond those provided for in the application of such State or States.

(B) STATE REVIEW AND SUBMISSION.—To ensure the consistency required under subsection (d) and the coordination required under subparagraph (A), an applicant that is a region must submit its application to each State of which any part is included in the region for review and concurrence prior to the submission of such application to the Secretary. The regional application shall be transmitted to the Secretary through each such State within 30 days of its receipt, unless the Governor of such a State notifies the Secretary, in writing, that such regional application is inconsistent with the State's homeland security plan and provides an explanation of the reasons therefor.

(C) DISTRIBUTION OF REGIONAL AWARDS.—If the Secretary approves a regional application, then the Secretary shall distribute a regional award to the State or States submitting the applicable regional application under subparagraph (B), and each such State shall, not later than the end of the 45-day period beginning on the date after receiving a regional award, pass through to the region all covered grant funds or resources purchased with such funds, except those funds necessary for the State to carry out its responsibilities with respect to such regional application: Provided, That in no such case shall the State or States pass through to the region less than 80 percent of the regional award.

(D) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS TO REGIONS.—Any State that receives a regional award under subparagraph (C) shall certify to the Secretary, by not later than 30 days after the expiration of the period described in subparagraph (C) with respect to the grant, that the State has made available to the region the

required funds and resources in accordance with subparagraph (C).

(E) DIRECT PAYMENTS TO REGIONS.—If any State fails to pass through a regional award to a region as required by subparagraph (C) within 45 days after receiving such award and does not request or receive an extension of such period, the region may petition the Secretary to receive directly the portion of the regional award that is required to be passed through to such region under subparagraph (C).

(F) REGIONAL LIAISONS.—A regional liaison designated under paragraph (4)(E)(iii) shall—

(i) coordinate with Federal, State, local, regional, and private officials within the region concerning terrorism preparedness;

(ii) develop a process for receiving input from Federal, State, local, regional, and private sector officials within the region to assist in the development of the regional application and to improve the region's access to covered grants; and

(iii) administer, in consultation with State, local, regional, and private officials within the region, covered grants awarded to the region.

(6) TRIBAL APPLICATIONS.—

(A) SUBMISSION TO THE STATE OR STATES.—To ensure the consistency required under subsection (d), an applicant that is a directly eligible tribe must submit its application to each State within the boundaries of which any part of such tribe is located for direct submission to the Department along with the application of such State or States.

(B) OPPORTUNITY FOR STATE COMMENT.—Before awarding any covered grant to a directly eligible tribe, the Secretary shall provide an opportunity to each State within the boundaries of which any part of such tribe is located to comment to the Secretary on the consistency of the tribe's application with the State's homeland security plan. Any such comments shall be submitted to the Secretary concurrently with the submission of the State and tribal applications.

(C) FINAL AUTHORITY.—The Secretary shall have final authority to determine the consistency of any application of a directly eligible tribe with the applicable State homeland security plan or plans, and to approve any application of such tribe. The Secretary shall notify each State within the boundaries of which any part of such tribe is located of the approval of an application by such tribe.

(D) TRIBAL LIAISON.—A tribal liaison designated under paragraph (4)(G) shall—

(i) coordinate with Federal, State, local, regional, and private officials concerning terrorism preparedness;

(ii) develop a process for receiving input from Federal, State, local, regional, and private sector officials to assist in the development of the application of such tribe and to improve the tribe's access to covered grants; and

(iii) administer, in consultation with State, local, regional, and private officials, covered grants awarded to such tribe.

(E) LIMITATION ON THE NUMBER OF DIRECT GRANTS.—The Secretary may make covered grants directly to not more than 20 directly eligible tribes per fiscal year.

(F) TRIBES NOT RECEIVING DIRECT GRANTS.—An Indian tribe that does not receive a grant directly under this section is eligible to receive funds under a covered grant from the State or States within the boundaries of which any part of such tribe is located, consistent with the homeland security plan of the State as described in subsection (c). If a State fails to pass through funds, the tribe may petition the Secretary to receive payment in the same manner as a local government.

(7) EQUIPMENT STANDARDS.—If an applicant for a covered grant proposes to upgrade or purchase, with assistance provided under the grant, new equipment or systems that do not meet or exceed any applicable national voluntary consensus standards, the applicant shall include in the application an explanation of why such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed such standards.

SEC. 2004. RISK-BASED EVALUATION AND PRIORITIZATION.

(a) FIRST RESPONDER GRANTS BOARD.—

(1) ESTABLISHMENT OF BOARD.—The Secretary shall establish a First Responder Grants Board, consisting of—

(A) the Secretary;

(B) the Under Secretary for Science and Technology;

(C) the Under Secretary for Policy;

(D) the Director of the Federal Emergency Management Agency;

(E) the Assistant Secretary for United States Immigration and Customs Enforcement;

(F) the Chief Intelligence Officer;

(G) the Administrator of the United States Fire Administration;

(H) the Department official with primary responsibility for preparedness;

(I) the Department official with primary responsibility for grants; and

(J) the Administrator of the Animal and Plant Health Inspection Service.

(2) CHAIRMAN.—

(A) IN GENERAL.—The Secretary shall be the Chairman of the Board.

(B) EXERCISE OF AUTHORITIES BY DEPUTY SECRETARY.—The Deputy Secretary of Homeland Security may exercise the authorities of the Chairman, if the Secretary so directs.

(b) FUNCTIONS OF BOARD MEMBERS.—The Under Secretaries, Assistant Secretaries, Administrators, and other officials referred to in subsection (a)(1) shall seek to ensure that the relevant expertise and input of their staff are available to and considered by the Board.

(c) PRIORITIZATION OF GRANT APPLICATIONS.—

(1) FACTORS TO BE CONSIDERED.—The Board shall evaluate and annually prioritize all pending applications for covered grants based upon—

(A) the degree to which they would, by achieving, maintaining, or enhancing the essential capabilities of the applicants on a nationwide basis, lessen the threat to, vulnerability of, and consequences for persons (including transient commuting and tourist populations) and critical infrastructure;

(B) prior acts of international terrorism;

(C) elevations in the threat alert level;

(D) the existence of significant ports of entry; and

(E) the most current risk assessment available of the threats of terrorism against the United States.

(2) CRITICAL INFRASTRUCTURE SECTORS.—The Board specifically shall consider threats of terrorism against the following critical infrastructure sectors in all areas of the United States, urban and rural:

(A) Agriculture and food.

(B) Banking and finance.

(C) Chemical industries.

(D) The defense industrial base.

(E) Emergency services.

(F) Energy.

(G) Government facilities.

(H) Postal and shipping.

(I) Public health and health care.

(J) Information technology.

(K) Telecommunications.

(L) Transportation systems.

(M) Water.

(N) Dams.

(O) Commercial facilities.

(P) National monuments and icons.

(Q) Commercial nuclear reactors, materials, and waste.

The order in which the critical infrastructure sectors are listed in this paragraph shall not be construed as an order of priority for consideration of the importance of such sectors.

(3) TYPES OF THREAT.—The Board specifically shall consider the following types of threat to the critical infrastructure sectors described in paragraph (2), and to populations in all areas of the United States, urban and rural:

(A) Biological threats.

(B) Nuclear threats.

(C) Radiological threats.

(D) Incendiary threats.

(E) Chemical threats.

(F) Explosives.

(G) Suicide bombers.

(H) Cyber threats.

(I) Any other threats based on proximity to specific past acts of terrorism or the known activity of any terrorist group.

The order in which the types of threat are listed in this paragraph shall not be construed as an order of priority for consideration of the importance of such threats.

(4) CONSIDERATION OF ADDITIONAL FACTORS.—The Board shall take into account any other specific threat to a population (including a transient commuting or tourist population) or critical infrastructure sector that the Board has determined to exist. In evaluating the threat to a population or critical infrastructure sector, the Board shall give greater weight to threats of terrorism based upon their specificity and credibility, including any pattern of repetition.

(5) RISK ANALYSIS AND ASSESSMENT.—Prior to evaluating and prioritizing all pending applications for covered grants, the Board shall provide an opportunity for applicants to provide information to the Board regarding the risk profile of the applicants' jurisdictions.

(6) COORDINATION.—The Board shall coordinate with State, local, regional, and tribal officials in establishing criteria for evaluating and prioritizing applications for covered grants.

(7) MINIMUM AMOUNTS.—After evaluating and prioritizing grant applications under paragraph (1), the Board shall ensure that, for each fiscal year—

(A) each of the States, other than the Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands, that has an approved State homeland security plan receives no less than 0.25 percent of the funds available for covered grants for that fiscal year for purposes of implementing its homeland security plan in accordance with the prioritization of needs under section 2003(c)(1)(D);

(B) each of the States, other than the Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands, that has an approved State homeland security plan and that meets one or both of the additional high-risk qualifying criteria under paragraph (8) receives no less than 0.45 percent of the funds available for covered grants for that fiscal year for purposes of implementing its homeland security plan in accordance with the prioritization of needs under section 2003(c)(1)(D);

(C) the Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands each receives no less than 0.08 percent of the funds available for covered grants for that fiscal year for purposes of implementing its approved State homeland security plan in accordance with the prioritization of needs under section 2003(c)(1)(D); and

(D) directly eligible tribes collectively receive no less than 0.08 percent of the funds available for covered grants for such fiscal year for purposes of addressing the needs identified in the applications of such tribes, consistent with the homeland security plan of each State within the boundaries of which any part of any such tribe is located, except that this clause shall not apply with respect to funds available for a fiscal year if the Secretary receives less than 5 applications for such fiscal year from such tribes under section 2003(e)(6)(A) or does not approve at least one such application.

(8) ADDITIONAL HIGH-RISK QUALIFYING CRITERIA.—For purposes of paragraph (7)(B), additional high-risk qualifying criteria consist of—

(A) having a significant international land border; or

(B) adjoining a body of water within North America through which an international boundary line extends.

(d) EFFECT OF REGIONAL AWARDS ON STATE MINIMUM.—Any regional award, or portion thereof, provided to a State under section 2003(e)(5)(C) shall not be considered in calculating the minimum State award under subsection (c)(7) of this section.

SEC. 2005. USE OF FUNDS.

(a) IN GENERAL.—A covered grant may be used for—

(1) purchasing or upgrading equipment, including computer software, to enhance terrorism preparedness;

(2) exercises to strengthen terrorism preparedness;

(3) training for prevention (including detection) of, preparedness for, response to, or recovery from attacks involving weapons of mass destruction, including training in the use of equipment and computer software;

(4) developing or updating State homeland security plans, risk assessments, mutual aid agreements, and emergency management plans to enhance terrorism preparedness;

(5) establishing or enhancing mechanisms for sharing terrorism threat information;

(6) systems architecture and engineering, program planning and management, strategy formulation and strategic planning, life-cycle systems design, product and technology evaluation, and prototype development for terrorism preparedness purposes;

(7) additional personnel costs resulting from—

(A) elevations in the threat alert level of the Homeland Security Advisory System by the Secretary, or a similar elevation in threat alert level issued by a State, region, or local government with the approval of the Secretary;

(B) travel to and participation in exercises and training in the use of equipment and on prevention activities; and

(C) the temporary replacement of personnel during any period of travel to and participation in exercises and training in the use of equipment and on prevention activities;

(8) the costs of equipment (including software) required to receive, transmit, handle, and store classified information;

(9) the costs of commercially available interoperable communications equipment (which, where applicable, is based on national, voluntary consensus standards) that the Secretary, in consultation with the Chairman of the Federal Communications Commission, deems best suited to facilitate interoperability, coordination, and integration between and among emergency communications systems, and that complies with prevailing grant guidance of the Department for interoperable communications;

(10) educational curricula development for first responders to ensure that they are prepared for terrorist attacks;

(11) training and exercises to assist public elementary and secondary schools in developing and implementing programs to instruct students regarding age-appropriate skills to prevent, prepare for, respond to, mitigate against, or recover from an act of terrorism;

(12) paying of administrative expenses directly related to administration of the grant, except that such expenses may not exceed 3 percent of the amount of the grant;

(13) paying for the conduct of any activity permitted under the Law Enforcement Terrorism Prevention Program, or any such successor to such program; and

(14) other appropriate activities as determined by the Secretary.

(b) PROHIBITED USES.—Funds provided as a covered grant may not be used—

(1) to supplant State or local funds;

(2) to construct buildings or other physical facilities, including barriers, fences, gates, and other such devices intended for the protection of critical infrastructure against potential attack, except those that are constructed under terms and conditions consistent with the requirements of section 611(j)(8) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5196(j)(8)), and the cost of which does not exceed the greater of—

(A) $1,000,000 per project; or

(B) such greater amount as may be approved by the Secretary, which may not exceed 10 percent of the total amount of the covered grant;

(3) to acquire land; or

(4) for any State or local government cost sharing contribution.

(c) PERSONNEL COSTS.—A State and local government may use a covered grant to pay costs of personnel dedicated exclusively to counterterrorism and intelligence activities (including detection of, collection and analysis of intelligence relating to, investigation of, prevention of, and interdiction of suspected terrorist activities), if the hiring of such personnel is consistent with an applicable State homeland security plan.

(d) MULTIPLE-PURPOSE FUNDS.—Nothing in this section shall be construed to preclude State and local governments from using covered grant funds in a manner that also enhances first responder preparedness for emergencies and disasters unrelated to acts of terrorism, if such use assists such governments in achieving essential capabilities for terrorism preparedness established by the Secretary.

(e) REIMBURSEMENT OF COSTS.—(1) In addition to the activities described in subsection (a), a covered grant may be used to provide a reasonable stipend to paid-on-call or volunteer first responders who are not otherwise compensated for travel to or participation in training covered by this section. Any such reimbursement shall not be considered compensation for purposes of rendering such a first responder an employee under the Fair Labor Standards Act of 1938 (29 U.S.C. 201 et seq.).

(2) An applicant for a covered grant may petition the Secretary for the reimbursement of the cost of any activity relating to prevention (including detection) of, preparedness for, response to, or recovery from acts of terrorism that is a Federal duty and usually performed by a Federal agency, and that is being performed by a State or local government (or both) under agreement with a Federal agency.

(f) ASSISTANCE REQUIREMENT.—The Secretary may not require that equipment paid for, wholly or in part, with funds provided as

a covered grant be made available for responding to emergencies in surrounding States, regions, and localities, unless the Secretary undertakes to pay the costs directly attributable to transporting and operating such equipment during such response.

(g) COST SHARING.—

(1) IN GENERAL.—The Federal share of the costs of an activity carried out with a covered grant to a State, region, or directly eligible tribe awarded after the 2-year period beginning on the date of the enactment of this section shall not exceed 75 percent.

(2) INTERIM RULE.—The Federal share of the costs of an activity carried out with a covered grant awarded before the end of the 2-year period beginning on the date of the enactment of this section shall be 100 percent.

(3) IN-KIND MATCHING.—Each recipient of a covered grant may meet the matching requirement under subparagraph (A) by making in-kind contributions of goods or services that are directly linked with the purpose for which the grant is made, as determined by the Secretary, including any necessary personnel overtime, contractor services, administrative costs, equipment fuel and maintenance, and rental space.

SECTION 1105 OF TITLE 31, UNITED STATES CODE

§ 1105. Budget contents and submission to Congress

(a) On or after the first Monday in January but not later than the first Monday in February of each year, the President shall submit a budget of the United States Government for the following fiscal year. Each budget shall include a budget message and summary and supporting information. The President shall include in each budget the following:

(1) * * *

* * * * * * *

[(33)**]** *(35)*(A)(i) * * *

(ii) with respect to subclauses (I) through (IV) of clause (i), amounts shall be provided by account for each program, project and activity; **[**and**]**

(iii) an estimate of expenditures for homeland security activities by State and local governments and the private sector for the prior fiscal year and the current fiscal year**[**.**]***; and*

(iv) a separate line item for each such fiscal year for expenditures by the Office of Counternarcotics Enforcement of the Department of Homeland Security.

* * * * * * *

SECTION 1202 OF THE 2002 SUPPLEMENTAL APPROPRIATIONS ACT FOR FURTHER RECOVERY FROM AND RESPONSE TO TERRORIST ATTACKS ON THE UNITED STATES

SEC. 1202. (a) The Federal Law Enforcement Training Center may, for a period ending not later than 5 years after the date of the **[**enactment of this Act**]** *enactment of the Department of Homeland Security Authorization Act for Fiscal Year 2007*, appoint and

maintain a cadre of up to [250] *350* Federal annuitants: (1) without regard to any provision of title 5, United States Code, which might otherwise require the application of competitive hiring procedures; and (2) who shall not be subject to any reduction in pay (for annuity allocable to the period of actual employment) under the provisions of section 8344 or 8468 of such title 5 or similar provision of any other retirement system for employees. A reemployed Federal annuitant as to whom a waiver of reduction under paragraph (2) applies shall not, for any period during which such waiver is in effect, be considered an employee for purposes of subchapter III of chapter 83 or chapter 84 of title 5, United States Code, or such other retirement system (referred to in paragraph (2)) as may apply.

* * * * * * *

SECTION 106 OF THE NATIONAL SECURITY ACT OF 1947

SEC. 106. (a) * * *

(b) CONCURRENCE OF DNI IN APPOINTMENTS TO POSITIONS IN THE INTELLIGENCE COMMUNITY.—(1) * * *

(2) Paragraph (1) applies to the following positions:

(A) * * *

* * * * * * *

[(I) The Assistant Secretary of Homeland Security for Information Analysis.]

(I) The Under Secretary of Homeland Security for Intelligence and Analysis.

* * * * * * *

SECTION 7306 OF THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

SEC. 7306. CRITICAL INFRASTRUCTURE AND READINESS ASSESSMENTS.

(a) FINDINGS.—Congress makes the following findings:

(1) Under section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121), the Department of Homeland Security, through the [Under Secretary for Information Analysis and Infrastructure Protection] *Under Secretary for Intelligence and Analysis*, has the responsibility—

(A) * * *

* * * * * * *

SECTION 319F–2 OF THE PUBLIC HEALTH SERVICE ACT

SEC. 319F–2. STRATEGIC NATIONAL STOCKPILE.

(a) * * *

* * * * * * *

(c) ADDITIONAL AUTHORITY REGARDING PROCUREMENT OF CERTAIN BIOMEDICAL COUNTERMEASURES; AVAILABILITY OF SPECIAL RESERVE FUND.—

(1) * * *

(2) DETERMINATION OF MATERIAL THREATS.—

[(A) MATERIAL THREAT.—The Homeland Security Secretary]

(A) MATERIAL THREAT.—

(i) IN GENERAL.—The Homeland Security Secretary, in consultation with the Secretary and the heads of other agencies as appropriate, shall on an ongoing basis—

[(i)] *(I)* assess current and emerging threats of chemical, biological, radiological, and nuclear agents; and

[(ii)] *(II)* determine which of such agents present a material threat against the United States population sufficient to affect national security.

(ii) USE OF EXISTING RISK ASSESSMENTS.—For the purpose of satisfying the requirements of clause (i) as expeditiously as possible, the Homeland Security Secretary shall, as practicable, utilize existing risk assessments that such Secretary considers credible.

(iii) ORDER OF ASSESSMENTS.—

(I) GROUPINGS TO FACILITATE ASSESSMENT OF COUNTERMEASURES.—In conducting threat assessments and determinations under clause (i) of chemical, biological, radiological, and nuclear agents, the Homeland Security Secretary shall, to the extent practicable and appropriate, consider the completion of such assessments and determinations for groups of agents toward the goal of facilitating the assessment of countermeasures under paragraph (3) by the Secretary of Health and Human Services.

(II) CATEGORIES OF COUNTERMEASURES.—The grouping of agents under subclause (I) by the Homeland Security Secretary shall be designed to facilitate assessments under paragraph (3) by the Secretary of Health and Human Services regarding the following two categories of countermeasures:

(aa) Countermeasures that may address more than one agent identified under clause (i)(II).

(bb) Countermeasures that may address adverse health consequences that are common to exposure to different agents.

(III) RULE OF CONSTRUCTION.—A particular grouping of agents pursuant to subclause (II) is not required under such subclause to facilitate assessments of both categories of countermeasures described in such subclause. A grouping may concern one category and not the other.

(iv) TIME FRAME FOR COMPLETION OF CERTAIN NATIONAL-SECURITY DETERMINATIONS.—With respect to chemical, biological, radiological, and nuclear agents

known to the Homeland Security Secretary as of the day before the date of the enactment of this Act, and which such Secretary considers to be capable of significantly affecting national security, such Secretary shall complete the determinations under clause (i)(II) not later than December 31, 2007.

(v) DEFINITION.—For purposes of this subparagraph, the term "risk assessment" means a scientific, technically-based analysis of agents that incorporates threat, vulnerability, and consequence information.

* * * * * * *

TITLE 49, UNITED STATES CODE

* * * * * * *

SUBTITLE I—DEPARTMENT OF TRANSPORTATION

* * * * * * *

CHAPTER 1—ORGANIZATION

* * * * * * *

§ 114. Transportation Security Administration

(a) * * *

* * * * * * *

(u) CIVIL PENALTIES AND ENFORCEMENT OF REGULATIONS AND ORDERS OF THE SECRETARY OF HOMELAND SECURITY UNDER THIS TITLE OTHER THAN CHAPTER 449.—

(1) APPLICATION.—This subsection applies to the enforcement of regulations prescribed, and orders issued, by the Secretary of Homeland Security under this title (other than chapter 449). Penalties for violation of regulations prescribed, and orders issued, by the Secretary of Homeland Security under chapter 449 of this title are provided under chapter 463 of this title.

(2) GENERAL PENALTY.—(A) A person is liable to the United States Government for a civil penalty of not more than $10,000 for a violation of a regulation prescribed, or order issued, by the Secretary of Homeland Security under an applicable provision of this title.

(B) A separate violation occurs under this paragraph for each day the violation continues.

(3) ADMINISTRATIVE IMPOSITION OF CIVIL PENALTIES.—(A) The Secretary of Homeland Security may impose a civil penalty for a violation of a regulation prescribed, or order issued, under an applicable provision of this title. The Secretary shall give written notice of the finding of a violation and the penalty.

(B) In a civil action to collect a civil penalty imposed by the Secretary under this paragraph, the issues of liability and the amount of the penalty may not be reexamined.

(C) Notwithstanding subparagraph (a) of this paragraph, the district courts of the United States have exclusive jurisdiction

of a civil action involving a penalty that the secretary initiates if—

(i) the amount in controversy is more than—

(I) $ 400,000 if the violation was committed by a person other than an individual or small business concern; or

(II) $ 50,000 if the violation was committed by an individual or small business concern;

(ii) the action is in rem or another action in rem based on the same violation has been brought; or

(iii) another action has been brought for an injunction based on the same violation.

(D) The maximum penalty the Secretary may impose under this paragraph is—

(i) $400,000 if the violation was committed by a person other than an individual or small business concern; or

(ii) $50,000 if the violation was committed by an individual or small business concern.

(4) COMPROMISE AND SETOFF.—(A) The Secretary may compromise the amount of a civil penalty imposed under this subsection.

(B) The Government may deduct the amount of a civil penalty imposed or compromised under this subsection from amounts it owes the person liable for the penalty.

(5) INVESTIGATIONS AND PROCEEDINGS.—The provisions set forth in chapter 461 of this title shall be applicable to investigations and proceedings brought under this subsection to the same extent that they are applicable to investigations and proceedings brought with respect to aviation security duties designated to be carried out by the Secretary.

(6) NONAPPLICATION.—Paragraphs (1) through (4) of this subsection do not apply to the following persons, who shall be subject to penalties as determined by the Secretary of Defense or the designee of the Secretary of Defense:

(A) The transportation of personnel or shipments of materials by contractors where the Department of Defense has assumed control and responsibility.

(B) A member of the armed forces of the United States when performing official duties.

(C) A civilian employee of the Department of Defense when performing official duties.

(7) LIMITATION.—For purposes of this subsection, the term "person" does not include an employee of the United States Postal Service when performing official duties.

(8) SMALL BUSINESS CONCERN DEFINED.—For purposes of this subsection, the term "small business concern" has the meaning given that term in section 3 of the Small Business Act (15 U.S.C. 632).

* * * * * * *

SUBTITLE VII—AVIATION PROGRAMS

* * * * * * *

PART A—AIR COMMERCE AND SAFETY

* * * * * * *

SUBPART III—SAFETY

* * * * * * *

CHAPTER 449—SECURITY

SUBCHAPTER I—REQUIREMENTS

Sec.
44901. Screening passengers and property.

* * * * * * *

SUBCHAPTER II—ADMINISTRATION AND PERSONNEL

* * * * * * *

[44938. Reports.]
44938. Transportation security report.

* * * * * * *

[44942. Performance goals and objectives.]

* * * * * * *

SUBCHAPTER I—REQUIREMENTS

§ 44901. Screening passengers and property

(a) * * *

* * * * * * *

(i) LIABILITY FOR SECURITY SCREENING INSPECTIONS.—

(1) LIMITATION FOR GOOD FAITH INSPECTIONS.—No officer or employee of the United States inspecting any person or property pursuant to section 44901 or 44903 shall be held liable for any civil damages as a result of such inspection if the officer or employee performed the inspection in good faith.

(2) LIMITATION ON STATUTORY CONSTRUCTION.—Nothing in this subsection shall be construed to impair any defense otherwise available to an officer or employee described in paragraph (1) under statute or common law, including any defense of absolute or qualified immunity.

(3) EXCLUSIVE REMEDY.—The exclusive remedy against the United States or its officers or employees for any damages arising from the loss, damage, detention, or negligent handling of property subject to security screening operations under section 44901 or 44903 shall be a claim pursuant to section 3723 of title 31, except that the maximum amount for which such a claim may be settled under section 3723(a) of title 31 shall be the same as the level established under section 254.4 of title 14, Code of Federal Regulations.

* * * * * * *

§ 44903. Air transportation security

(a) * * *

* * * * * * *

(j) SHORT-TERM ASSESSMENT AND DEPLOYMENT OF EMERGING SECURITY TECHNOLOGIES AND PROCEDURES.—

(1) * * *

(2) COMPUTER-ASSISTED PASSENGER PRESCREENING SYSTEM.—

(A) * * *

* * * * * * *

(E) AIRCRAFT CHARTER CUSTOMER AND LESSEE PRESCREENING.—

(i) IN GENERAL.—Not later than 90 days after the date on which the Assistant Secretary assumes the performance of the advanced passenger prescreening function under subparagraph (C)(ii), the Assistant Secretary shall establish a process by which operators of aircraft to be used in charter air transportation with a maximum *certificated* takeoff weight greater than 12,500 pounds and lessors of aircraft with a maximum *certificated* takeoff weight greater than 12,500 pounds may—

(I) request the Department of Homeland Security to use the advanced passenger prescreening system to compare information about any individual seeking to charter an aircraft with a maximum *certificated* takeoff weight greater than 12,500 pounds, any passenger proposed to be transported aboard such aircraft, and any individual seeking to lease an aircraft with a maximum *certificated* takeoff weight greater than 12,500 pounds to the automatic selectee and no fly lists, utilizing all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government; and

(II) refuse to charter or lease an aircraft with a maximum *certificated* takeoff weight greater than 12,500 pounds to or transport aboard such aircraft any persons identified on such watch list.

* * * * * * *

§ 44920. Security screening opt-out program

(a) * * *

* * * * * * *

(h) EMERGENCY SUPPLEMENTAL SCREENING.—The Secretary of Homeland Security may establish a program under which the screening of passengers and property at an airport under section 44901 may be supplemented for periods of limited duration in case of emergencies, such as natural disasters, terrorist acts, or threats to national security, by the screening personnel of a qualified private screening company in accordance with subsections (c) and (d) under a contract entered into with the Secretary.

§ 44921. Federal flight deck officer program

(a) ESTABLISHMENT.—The [Under Secretary of Transportation for Security] *Assistant Secretary of Homeland Security (Transportation Security Administration)* shall establish a program to deputize volunteer pilots of air carriers providing air transportation or intrastate air transportation as Federal law enforcement officers to de-

fend the flight decks of aircraft of such air carriers against acts of criminal violence or air piracy. Such officers shall be known as "Federal flight deck officers".

(b) PROCEDURAL REQUIREMENTS.—

(1) IN GENERAL.—Not later than 3 months after the date of enactment of this section, the [Under Secretary] *Assistant Secretary* shall establish procedural requirements to carry out the program under this section.

(2) COMMENCEMENT OF PROGRAM.—Beginning 3 months after the date of enactment of this section, the [Under Secretary] *Assistant Secretary* shall begin the process of training and deputizing pilots who are qualified to be Federal flight deck officers as Federal flight deck officers under the program.

(3) ISSUES TO BE ADDRESSED.—The procedural requirements established under paragraph (1) shall address the following issues:

(A) * * *

* * * * * * *

(M) Any other issues that the [Under Secretary] *Assistant Secretary* considers necessary.

(N) The [Under Secretary's] *Assistant Secretary's* decisions regarding the methods for implementing each of the foregoing procedural requirements shall be subject to review only for abuse of discretion.

(4) PREFERENCE.—In selecting pilots to participate in the program, the [Under Secretary] *Assistant Secretary* shall give preference to pilots who are former military or law enforcement personnel.

* * * * * * *

(6) NOTICE TO CONGRESS.—The [Under Secretary] *Assistant Secretary* shall provide notice to the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate after completing the analysis required by paragraph (3)(E).

(7) MINIMIZATION OF RISK.—If the [Under Secretary] *Assistant Secretary* determines as a result of the analysis under paragraph (3)(E) that there is a significant risk of the catastrophic failure of an aircraft as a result of the discharge of a firearm, the [Under Secretary] *Assistant Secretary* shall take such actions as may be necessary to minimize that risk.

(c) TRAINING, SUPERVISION, AND EQUIPMENT.—

(1) IN GENERAL.—The [Under Secretary] *Assistant Secretary* shall only be obligated to provide the training, supervision, and equipment necessary for a pilot to be a Federal flight deck officer under this section at no expense to the pilot or the air carrier employing the pilot.

(2) TRAINING.—

(A) IN GENERAL.—The [Under Secretary] *Assistant Secretary* shall base the requirements for the training of Federal flight deck officers under subsection (b) on the training standards applicable to Federal air marshals; except that the [Under Secretary] *Assistant Secretary* shall take

into account the differing roles and responsibilities of Federal flight deck officers and Federal air marshals.

* * * * * * *

(C) TRAINING IN USE OF FIREARMS.—

(i) STANDARD.—In order to be deputized as a Federal flight deck officer, a pilot must achieve a level of proficiency with a firearm that is required by the [Under Secretary] *Assistant Secretary*. Such level shall be comparable to the level of proficiency required of Federal air marshals.

(ii) CONDUCT OF TRAINING.—The training of a Federal flight deck officer in the use of a firearm may be conducted by the [Under Secretary] *Assistant Secretary* or by a firearms training facility approved by the [Under Secretary] *Assistant Secretary*.

(iii) REQUALIFICATION.—The [Under Secretary] *Assistant Secretary* shall require a Federal flight deck officer to requalify to carry a firearm under the program. Such requalification shall occur at an interval required by the [Under Secretary] *Assistant Secretary*.

(3) DATES OF TRAINING.—The Assistant Secretary shall ensure that a pilot who is eligible to receive Federal flight deck officer training is offered, to the maximum extent practicable, a choice of training dates and is provided at least 30 days advance notice of the dates.

(4) TRAVEL TO TRAINING FACILITIES.—The Assistant Secretary shall establish a program to improve travel access to Federal flight deck officer training facilities through the use of charter flights or improved scheduled air carrier service.

(5) REQUALIFICATION AND RECURRENT TRAINING.—

(A) STANDARDS.—The Assistant Secretary shall establish qualification standards for facilities where Federal flight deck officers can receive requalification and recurrent training.

(B) LOCATIONS.—The Assistant Secretary shall provide for requalification and recurrent training at geographically diverse facilities, including Federal, State, and local law enforcement and government facilities, and private training facilities that meet the qualification standards established under subparagraph (A).

(6) COSTS OF TRAINING.—

(A) IN GENERAL.—The Assistant Secretary shall provide Federal flight deck officer training, requalification training, and recurrent training to eligible pilots at no cost to the pilots or the air carriers that employ the pilots.

(B) TRANSPORTATION AND EXPENSES.—The Assistant Secretary may provide travel expenses to a pilot receiving Federal flight deck officer training, requalification training, or recurrent training.

(7) COMMUNICATIONS.—Not later than 180 days after the date of enactment of this paragraph, the Assistant Secretary shall establish a secure means for personnel of the Transportation Security Administration to communicate with Federal flight deck officers, and for Federal flight deck officers to communicate

with each other, in support of the mission of such officers. Such means of communication may include a secure Internet website.

(d) DEPUTIZATION.—

(1) IN GENERAL.—The [Under Secretary] *Assistant Secretary* may deputize, as a Federal flight deck officer under this section, a pilot who submits to the [Under Secretary] *Assistant Secretary* a request to be such an officer and whom the [Under Secretary] *Assistant Secretary* determines is qualified to be such an officer.

(2) QUALIFICATION.—A pilot is qualified to be a Federal flight deck officer under this section if—

(A) the pilot is employed by an air carrier;

(B) the [Under Secretary] *Assistant Secretary* determines (in the [Under Secretary's] *Assistant Secretary's* discretion) that the pilot meets the standards established by the [Under Secretary] *Assistant Secretary* for being such an officer; and

(C) the [Under Secretary] *Assistant Secretary* determines that the pilot has completed the training required by the [Under Secretary] *Assistant Secretary*.

(3) DEPUTIZATION BY OTHER FEDERAL AGENCIES.—The [Under Secretary] *Assistant Secretary* may request another Federal agency to deputize, as Federal flight deck officers under this section, those pilots that the [Under Secretary] *Assistant Secretary* determines are qualified to be such officers.

[(4) REVOCATION.—The Under Secretary may, (in the Under Secretary's discretion) revoke the deputization of a pilot as a Federal flight deck officer if the Under Secretary finds that the pilot is no longer qualified to be such an officer.]

(4) REVOCATION.—

(A) ORDERS.—The Assistant Secretary may issue, for good cause, an order revoking the deputization of a Federal flight deck officer under this section. The order shall include the specific reasons for the revocation.

(B) HEARINGS.—An individual who is adversely affected by an order of the Assistant Secretary under subparagraph (A) is entitled to a hearing on the record. When conducting a hearing under this subparagraph, the administrative law judge shall not be bound by findings of fact or interpretations of laws and regulations of the Assistant Secretary.

(C) APPEALS.—An appeal from a decision of an administrative law judge as a result of a hearing under subparagraph (B) shall be made to the Secretary of Homeland Security or the Secretary's designee.

(D) JUDICIAL REVIEW OF A FINAL ORDER.—The determination and order of the Secretary revoking the deputization of a Federal flight deck officer under this section shall be final and conclusive unless the individual against whom such an order is issued files an application for judicial review under subchapter II of chapter 5 of title 5 (popularly known as the Administrative Procedure Act) within 60 days of entry of such order in the appropriate United States court of appeals.

* * * * * * *

(f) AUTHORITY TO CARRY FIREARMS.—

(1) IN GENERAL.—The [Under Secretary] *Assistant Secretary* shall authorize a Federal flight deck officer to carry a firearm while engaged in providing air transportation or intrastate air transportation. Notwithstanding subsection (c)(1), the officer may purchase a firearm and carry that firearm aboard an aircraft of which the officer is the pilot in accordance with this section if the firearm is of a type that may be used under the program.

* * * * * * *

(3) CARRYING FIREARMS OUTSIDE UNITED STATES.—In consultation with the Secretary of State, the [Under Secretary] *Assistant Secretary* may take such action as may be necessary to ensure that a Federal flight deck officer may carry a firearm in a foreign country whenever necessary to participate in the program.

(4) PILOT PROGRAM.—

(A) IN GENERAL.—Not later than 90 days after the date of enactment of this paragraph, the Assistant Secretary shall implement a pilot program to allow pilots participating in the Federal flight deck officer program to transport their firearms on their persons. The Assistant Secretary may prescribe any training, equipment, or procedures that the Assistant Secretary determines necessary to ensure safety and maximize weapon retention.

(B) REVIEW.—Not later than 1 year after the date of initiation of the pilot program, the Assistant Secretary shall conduct a review of the safety record of the pilot program and transmit a report on the results of the review to Congress.

(C) OPTION.—If the Assistant Secretary as part of the review under subparagraph (B) determines that the safety level obtained under the pilot program is comparable to the safety level determined under existing methods of pilots carrying firearms on aircraft, the Assistant Secretary shall allow all pilots participating in the Federal flight deck officer program the option of carrying their firearm on their person subject to such requirements as the Assistant Secretary determines appropriate.

(g) AUTHORITY TO USE FORCE.—Notwithstanding section 44903(d), the [Under Secretary] *Assistant Secretary* shall prescribe the standards and circumstances under which a Federal flight deck officer may use, while the program under this section is in effect, force (including lethal force) against an individual in the defense of the flight deck of an aircraft in air transportation or intrastate air transportation.

* * * * * * *

(i) PROCEDURES FOLLOWING ACCIDENTAL DISCHARGES.—If an accidental discharge of a firearm under the pilot program results in the injury or death of a passenger or crew member on an aircraft, the [Under Secretary] *Assistant Secretary—*

(1) shall revoke the deputization of the Federal flight deck officer responsible for that firearm if the [Under Secretary] *Assistant Secretary* determines that the discharge was attributable to the negligence of the officer; and

(2) if the [Under Secretary] *Assistant Secretary* determines that a shortcoming in standards, training, or procedures was responsible for the accidental discharge, the [Under Secretary] *Assistant Secretary* may temporarily suspend the program until the shortcoming is corrected.

* * * * * * *

SUBCHAPTER II—ADMINISTRATION AND PERSONNEL

* * * * * * *

§ 44938. [Reports] *Transportation security report*

[(a) TRANSPORTATION SECURITY.—]Not later than March 31 of each year, the Secretary of Transportation shall submit to Congress a report on transportation security with recommendations the Secretary considers appropriate. [The report shall be prepared in conjunction with the biennial report the Under Secretary of Transportation Security submits under subsection (b) of this section in each year the Under Secretary submits the biennial report, but may not duplicate the information submitted under subsection (b) or section 44907(a)(3) of this title.] The Secretary may submit the report in classified and unclassified parts. The report shall include—

(1) * * *

* * * * * * *

(9) an assessment of financial and staffing requirements, and attainment of existing staffing goals, for carrying out duties and powers of the Under Secretary related to security; [and]

(10) appropriate legislative and regulatory recommendations[.]*;*

(11) an assessment of the effectiveness of procedures under section 44901;

(12) a summary of the assessments conducted under section 44907(a)(1) and (2); and

(13) an assessment of the steps being taken, and the progress being made, in ensuring compliance with section 44906 for each foreign air carrier security program at airports outside the United States—

(A) at which the Secretary decides that foreign security liaison officers are necessary for air transportation security; and

(B) for which extraordinary security measures are in place.

[(b) SCREENING AND FOREIGN AIR CARRIER AND AIRPORT SECURITY.—The Under Secretary shall submit biennially to Congress a report—

[(1) on the effectiveness of procedures under section 44901 of this title;

[(2) that includes a summary of the assessments conducted under section 44907(a)(1) and (2) of this title; and

[(3) that includes an assessment of the steps being taken, and the progress being made, in ensuring compliance with section 44906 of this title for each foreign air carrier security program at airports outside the United States—

[(A) at which the Under Secretary decides that Foreign Security Liaison Officers are necessary for air transportation security; and

[(B) for which extraordinary security measures are in place.]

§ 44939. Training to operate certain aircraft

(a) * * *

* * * * * * *

(f) NONAPPLICABILITY TO CERTAIN FOREIGN MILITARY PILOTS.—The procedures and processes required by subsections (a) through (d) *and (g)* shall not apply to a foreign military pilot endorsed by the Department of Defense for flight training in the United States and seeking training described in subsection (e) in the United States.

(g) FEE.—

(1) * * *

(2) RECURRENT TRAINING.—The Secretary may assess a fee for a threat assessment to determine that an alien as defined in this section, or any other individual specified by the Secretary, applying for recurrent training in the operation of any aircraft having a maximum certificated takeoff weight of more than 12,500 pounds is properly identified and has not since the time of any prior threat assessment conducted pursuant to this section become a present risk to aviation or national security. If the Secretary determines that such individual is a present risk to aviation or national security the Secretary shall immediately notify the person providing the training of the determination and that person shall not provide the training or if such training has commenced that person shall immediately terminate the training. Such fee shall not exceed the amount assessed under paragraph (1) and shall be promulgated by notice in the Federal Register.

[(2)] *(3)* OFFSET.—Notwithstanding section 3302 of title 31, any fee collected under this section—

(A) shall be credited to the account in the Treasury from which the expenses were incurred and shall be available to the Secretary for those expenses; and

(B) shall remain available until expended.

* * * * * * *

[§ 44942. Performance goals and objectives

[(a) SHORT TERM TRANSITION.—

[(1) IN GENERAL.—Within 180 days after the date of enactment of the Aviation and Transportation Security Act, the Under Secretary for Transportation Security may, in consultation with Congress—

[(A) establish acceptable levels of performance for aviation security, including screening operations and access control, and

[(B) provide Congress with an action plan, containing measurable goals and milestones, that outlines how those levels of performance will be achieved.

[(2) BASICS OF ACTION PLAN.—The action plan shall clarify the responsibilities of the Transportation Security Administration, the Federal Aviation Administration and any other agency or organization that may have a role in ensuring the safety and security of the civil air transportation system.

[(b) LONG-TERM RESULTS-BASED MANAGEMENT.—

[(1) PERFORMANCE PLAN AND REPORT.—

[(A) PERFORMANCE PLAN.—

[(i) Each year, consistent with the requirements of the Government Performance and Results Act of 1993 (GPRA), the Secretary and the Under Secretary for Transportation Security shall agree on a performance plan for the succeeding 5 years that establishes measurable goals and objectives for aviation security. The plan shall identify action steps necessary to achieve such goals.

[(ii) In addition to meeting the requirements of GPRA, the performance plan should clarify the responsibilities of the Secretary, the Under Secretary for Transportation Security and any other agency or organization that may have a role in ensuring the safety and security of the civil air transportation system.

[(B) PERFORMANCE REPORT.—Each year, consistent with the requirements of GPRA, the Under Secretary for Transportation Security shall prepare and submit to Congress an annual report including an evaluation of the extent goals and objectives were met. The report shall include the results achieved during the year relative to the goals established in the performance plan.]

* * * * * * *

SUBPART IV—ENFORCEMENT AND PENALTIES

* * * * * * *

CHAPTER 463—PENALTIES

* * * * * * *

§ 46301. Civil penalties

(a) GENERAL PENALTY.—(1) * * *

* * * * * * *

(4) Aviation security violations-Notwithstanding paragraph (1) of this subsection, the maximum civil penalty for violating chapter 449 [or another requirement under this title administered by the Under Secretary of Transportation for Security] shall be $10,000; except that the maximum civil penalty shall be $25,000 in the case of a person operating an aircraft for the transportation of passengers or property for compensation (except an individual serving as an airman).

* * * * * * *

PART C—FINANCING

* * * * * * *

CHAPTER 483—AVIATION SECURITY FUNDING

* * * * * * *

[§ 48301. Aviation security funding

[(a) IN GENERAL.—There are authorized to be appropriated for fiscal years 2002, 2003, 2004, 2005, and 2006 such sums as may be necessary to carry out chapter 449 and related aviation security activities under this title. Any amounts appropriated pursuant to this section for fiscal year 2002 shall remain available until expended.

[(b) GRANTS FOR AIRCRAFT SECURITY.—There is authorized to be appropriated $500,000,000 for fiscal year 2002 to the Secretary of Transportation to make grants to or other agreements with air carriers (including intrastate air carriers) to—

[(1) fortify cockpit doors to deny access from the cabin to the pilots in the cockpit;

[(2) provide for the use of video monitors or other devices to alert the cockpit crew to activity in the passenger cabin;

[(3) ensure continuous operation of the aircraft transponder in the event the crew faces an emergency; and

[(4) provide for the use of other innovative technologies to enhance aircraft security.]

§ 48301. Aviation security funding

There are authorized to be appropriated for fiscal years 2006, 2007, 2008, 2009, and 2010 such sums as may be necessary to carry out chapter 449 and related aviation security activities under this title.

* * * * * * *

AVIATION AND TRANSPORTATION SECURITY ACT

TITLE I—AVIATION SECURITY

* * * * * * *

SEC. 109. ENHANCED SECURITY MEASURES.

(a) * * *

[(b) REPORT.—Not later than 6 months after the date of enactment of this Act, and annually thereafter until the Under Secretary has implemented or decided not to take each of the actions specified in subsection (a), the Under Secretary shall transmit to Congress a report on the progress of the Under Secretary in evaluating and taking such actions, including any legislative recommendations that the Under Secretary may have for enhancing transportation security.]

* * * * * * *

SEC. 137. RESEARCH AND DEVELOPMENT OF AVIATION SECURITY TECHNOLOGY.

(a) FUNDING.—To augment the programs authorized in section 44912(a)(1) of title 49, United States Code, there is authorized to be appropriated an additional $50,000,000 for each of fiscal years

[2002 through 2006] *2006 through 2010* and such sums as are necessary for each fiscal year thereafter to the Transportation Security Administration, for research, development, testing, and evaluation of the following technologies which may enhance [aviation] *transportation* security in the future. Grants to industry, academia, and Government entities to carry out the provisions of this section shall be available for fiscal years [2002 and 2003] *2006 through 2010* for—

(1) * * *

* * * * * * *

(4) acceleration of research, development, testing, and evaluation of threats carried on persons boarding [aircraft] *transportation vehicles* or entering secure areas, including detection of weapons, explosives, and components of weapons of mass destruction;

(5) acceleration of research, development, testing and evaluation of integrated systems of [airport] *transportation* security enhancement, including quantitative methods of assessing security factors at airports *and other transportation terminals and ports* selected for testing such systems;

(6) expansion of the existing program of research, development, testing, and evaluation of improved methods of education, training, and testing of key [airport] *transportation* security personnel; and

(7) acceleration of research, development, testing, and [evaluation of aircraft] *evaluation of conveyance* hardening materials, and techniques to reduce the [vulnerability of aircraft] *vulnerability of conveyances* to terrorist attack.

(b) GRANTS.—Grants awarded under this subtitle shall identify potential outcomes of the research, and propose a method for quantitatively assessing effective increases in security upon completion of the research program. At the conclusion of each grant, the grant recipient shall submit a final report to the [Transportation Security Administration] *Department of Homeland Security* that shall include sufficient information to permit the Under Secretary of Transportation for Security to prepare a cost-benefit analysis of potential improvements to airport security based upon deployment of the proposed technology. The Under Secretary shall begin awarding grants under this subtitle within 90 days of the date of enactment of this Act.

* * * * * * *

VISION 100—CENTURY OF AVIATION REAUTHORIZATION ACT

* * * * * * *

TITLE VI—AVIATION SECURITY

* * * * * * *

[SEC. 607. CAPPS2.

[(a) IN GENERAL.—The Under Secretary for Border and Transportation Security of the Department of Homeland Security shall

not implement, on other than a test basis, the computer assisted passenger prescreening system (commonly known as and in this section referred to as "CAPPS2") until the Under Secretary provides to Congress a certification that—

[(1) a procedure is established enabling airline passengers, who are delayed or prohibited from boarding a flight because CAPPS2 determined that they might pose a security threat, to appeal such determination and correct information contained in CAPPS2;

[(2) the error rate of the Government and private data bases that will be used to both establish identity and assign a risk level to a passenger under CAPPS2 will not produce a large number of false positives that will result in a significant number of passengers being mistaken as a security threat;

[(3) the Under Secretary has demonstrated the efficacy and accuracy of all search tools in CAPPS2 and has demonstrated that CAPPS2 can make an accurate predictive assessment of those passengers who would constitute a security threat;

[(4) the Secretary of Homeland Security has established an internal oversight board to oversee and monitor the manner in which CAPPS2 is being implemented;

[(5) the Under Secretary has built in sufficient operational safeguards to reduce the opportunities for abuse;

[(6) substantial security measures are in place to protect CAPPS2 from unauthorized access by hackers or other intruders;

[(7) the Under Secretary has adopted policies establishing effective oversight of the use and operation of the system; and

[(8) there are no specific privacy concerns with the technological architecture of the system.

[(b) GAO REPORT.—Not later than 90 days after the date on which certification is provided under subsection (a), the Comptroller General shall submit a report to the Committees on Appropriations of the House of Representatives and the Senate, the Committee on Transportation and Infrastructure of the House of Representatives, and the Committee on Commerce, Science and Transportation of the Senate that assesses the impact of CAPPS2 on the issues listed in subsection (a) and on privacy and civil liberties. The report shall include any recommendations for practices, procedures, regulations, or legislation to eliminate or minimize adverse effect of CAPPS2 on privacy, discrimination, and other civil liberties.

[SEC. 608. REPORT ON PASSENGER PRESCREENING PROGRAM.

[(a) IN GENERAL.—Within 90 days after the date of enactment of this Act, the Secretary of Homeland Security, after consultation with the Attorney General, shall submit a report in writing to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Transportation and Infrastructure on the potential impact of the Transportation Security Administration's proposed Computer Assisted Passenger Prescreening system, commonly known as CAPPS2, on the privacy and civil liberties of United States citizens.

[(b) SPECIFIC ISSUES TO BE ADDRESSED.—The report shall address the following:

[(1) Whether and for what period of time data gathered on individual travelers will be retained, who will have access to

such data, and who will make decisions concerning access to such data.

[(2) How the Transportation Security Administration will treat the scores assigned to individual travelers to measure the likelihood they may pose a security threat, including how long such scores will be retained and whether and under what circumstances they may be shared with other governmental, nongovernmental, or commercial entities.

[(3) The role airlines and outside vendors or contractors will have in implementing and operating the system, and to what extent will they have access, or the means to obtain access, to data, scores, or other information generated by the system.

[(4) The safeguards that will be implemented to ensure that data, scores, or other information generated by the system will be used only as officially intended.

[(5) The procedures that will be implemented to mitigate the effect of any errors, and what procedural recourse will be available to passengers who believe the system has wrongly barred them from taking flights.

[(6) The oversight procedures that will be implemented to ensure that, on an ongoing basis, privacy and civil liberties issues will continue to be considered and addressed with high priority as the system is installed, operated, and updated.]

* * * * * * *

MINORITY VIEWS

The Democratic Members of the Committee on Homeland Security began 2006 looking forward to a comprehensive and timely FY 2007 authorization process, culminating in legislation that would inform, provide guidance to and set funding priorities for the Appropriations Committee on programmatic activities in the Department of Homeland Security. A fundamental responsibility of an authorizing committee is to ensure the passage of an authorization bill, no matter the admittedly problematic jurisdictional waters that must be navigated by a relatively new Committee. Only by exerting its full jurisdictional authorities will this Committee be able to ensure that the Department of Homeland Security has the necessary programmatic oversight, management tools and funding to address America's security priorities.

From its establishment in 2003, the Department has received little of the direction and oversight from Congress deserving of an agency of its size and budget. Despite the appearance of Department officials at hearings before multiple committees of overlapping jurisdiction, Congress has failed to provide the Department with coherent guidance. This lack of congressional guidance and oversight became all too clear last year during Hurricane Katrina.

The FY 2007 Department of Homeland Security Authorization bill is of particular interest to Democratic Members because of the many Department failures in leadership, management, coordination and emergency response revealed during the course of Hurricane Katrina. An authorization bill also appeared an appropriate vehicle in which to address structural changes in the Department.

To this end, Democratic Members wrote to Chairman Peter T. King (R-NY) early this year expressing concern about an abbreviated authorization process and a desire to complete a bill prior to the beginning of the appropriations process.[1] If the Armed Services Committee was able to produce an authorization bill for the Department of Defense every single year, even during the height of the Cold War, then surely the Committee on Homeland Security should be equal to such a task during the War on Terror.

Unfortunately, H.R. 5814 is by no means a comprehensive, or even a particularly timely authorization bill, since Committee markup comes more than a month after H.R. 5441, the FY 2007 Appropriations bill, was passed by the House of Representatives.[2] The Senate too has already voted on the Department of Homeland Security appropriations bill.[3] H.R. 5814's limited content is somewhat mitigated by prior passage of bills from this committee on

[2] H.R. 5441, the Homeland Security Authorization bill was passed by the House of Representatives on June 6, 2006.

[3] H.R. 5441 was passed by the Senate on July 13, 2006.

[4] H.R. 1544 passed the House of Representatives by recorded vote: 409–10 (Roll No. 170) on May 12, 2005.

port security, the restructuring of the Federal Emergency Management Administration, international technology cooperation and securing the handling of ammonia nitrate. With the exception of H.R. 4954, the Security and Accountability for Every Port Act (SAFE Port Act), however, NONE of these bills has yet passed the House of Representatives. Early action, especially with regard to an authorization bill, is critical if an authorizing committee is not to cede those responsibilities, however inadvertently, to the Appropriations Committee.

Yet despite its delayed arrival in full Committee, and its fairly limited content, H.R. 5814 is a good bipartisan bill. Introduced by Chairman King, Ranking Member, Representative Bennie G. Thompson (MS–02), Chairman of the Management, Integration and Oversight Subcommittee, Representative Mike Rogers (AL–03) and Ranking Member, Representative Kendrick B. Meek (FL–17), this bill and the Amendment in the Nature of a Substitute offered by Chairman King include important substantive legislative and oversight provisions that should substantially improve the performance of and set priorities for the Department of Homeland Security. Specifically, H.R. 5814 and the Amendment in the Nature of a Substitute address significant concerns in the area of transportation security, intelligence and information sharing and perhaps most significantly contracting and procurement.

We sincerely appreciate the bipartisan spirit which marked the authorization process and the inclusion of Democratic ideas which constitute the majority of the text of H.R. 5814, and the Amendment in the Nature of a Substitute.

MANAGEMENT PRIORITIES

H.R. 5814 flattens the management structure at the Department by eliminating the Management Directorate. This proposal, which was originally offered by Representative Kendrick B. Meek (FL–17) during the mark-up of the FY 2006 authorization bill, will provide the Chief Financial Officer, Chief Procurement Officer, Chief Information Officer, Chief Human Resources Officer, Chief Administrative Officer, and the Chief Security Officer with more access to the Secretary and with more authority over their counterparts in the Department's lower-level agencies. The bill also makes a number of other management reforms, most of which were proposed in some form by Democrats on the Management, Integration & Oversight Subcommittee, including creating a procurement training curriculum for contracting officials and program managers at the Department, strengthening the SAFETY Act office, and requiring investigations of large expenditures in the new border security SBI—net program. The bill includes a number of personnel reforms, including setting a cap on training costs for Border Patrol agents, and providing more recruitment and retention incentives for Border Patrol agents. Additionally, the bill strengthens canine standards.

Protecting the nation's critical infrastructure is one of the core missions of the Department. Since the vast majority (85%) of the nation's critical infrastructure is privately owned, in order to fulfill this mission, it is imperative that the Department be able to share threat information with the owners and operators of critical infrastructure. This information sharing has been hampered in the past

because private sector entities do not, in most cases, possess the necessary security clearances needed to receive this information. We must increase the speed with which the necessary background checks are done so that these clearances can be granted, and we are glad that the Committee has agreed to direct the Chief Security Officer to make this a priority.

Additionally, we appreciate the inclusion of provisions offered by Representative Meek in the base bill which would require the Secretary to report on the feasibility of devising an exercise program to test the capabilities of Federal, state and local governments to detect and prevent fraud, waste, and abuse during an emergency response. It is our belief that individuals who have the responsibility for preventing fraud should be involved in a disaster response upon its onset and, thus, should be involved in national exercise programs.

The bill directs the Secretary to add a new support annex to the National Response Plan that addresses emergency contracting. Hurricane Katrina showed more than just how unprepared the Department and FEMA were for a major catastrophe, it showed how unprepared the entire government was for such an event. This support annex will detail how federal agencies are to coordinate procurements and ensure rapid, cost effective delivery of goods and services to disaster victims, and will help to ensure that the waste, fraud, and abuse that occurred after Hurricane Katrina is not repeated.

TRANSPORTATION SECURITY

H.R. 5814 also includes several aviation security provisions, including a provision offered by Representative Edward J. Markey (MA–7), prohibiting scissors and tools, including screwdrivers, wrenches and pliers, from being carried aboard a passenger aircraft, language offered by Representative James R. Langevin (RI–2) requiring Transportation Security Administration (TSA) to issue regulations for security at foreign repair stations, and a provision offered by Representative Nita M. Lowey (NY–18), requiring TSA to develop within a year a plan to screen all airport workers.

We are pleased to see that language from H.R. 5714, the Rail and Public Transportation Security Act of 2006, introduced by Homeland Security Committee members, Representatives Thompson, Loretta Sanchez (CA–47), Donna Christensen (VI), Peter DeFazio (OR–4), Zoe Lofgren (CA–16), Eleanor Holmes Norton (DC), Kendrick Meek (FL–17), and Sheila Jackson Lee (TX–18) in June was incorporated into the bill. Specifically, the bill included language concerning security plans, vulnerability assessments, grants, exercises, training, and information sharing. Unfortunately, the Department of Homeland Security has yet to focus attention on rail and mass transit security.

We are disappointed, however, that key pieces of the Rail and Public Transportation Security Act of 2006 were not included in the Department of Homeland Security Authorization Act. Security training for front-line rail and public transportation employees should be mandatory. The language included in this bill merely requires the Department of Homeland Security to develop and issue guidance. Second, the security plans required by the Authorization

bill should be reviewed, approved, and enforced by the Department of Homeland Security, a requirement that did not make it into the authorization bill. The creation of a security plan is not enough. These security plans must be reviewed, approved, and enforced—the lives of the millions of people ride our nation's rail and public transportation systems everyday are at risk as long as these requirements go unmet. Finally, whistleblower protections must be provided to front-line rail and public transportation employees so that employers cannot retaliate against employees who report security risks.

INTELLIGENCE

Democrats fully support the provisions of H.R. 5814 addressing the Department's intelligence and information sharing efforts. With only minor technical changes, Title V encompasses all of the provisions included in four bipartisan pieces of legislation—H.R. 5001, H.R. 5002, H.R. 5003, and H.R. 5004—introduced by Chairman Rob Simmons and Ranking Member Zoe Lofgren on March 16, 2006, and later reported out of the Subcommittee on Intelligence, Information Sharing & Terrorism Risk Assessment on a bipartisan basis on March 29, 2006.

During his Second Stage Review testimony before the Committee on July 13, 2005, Secretary Chertoff announced the creation of the Office of Intelligence and Analysis (I&A) and the Chief Intelligence Officer (CINT) position. The Secretary described I&A as an analytic entity "empowered to coordinate activities and fuse information from all intelligence offices" within the Department that accordingly would be able to create a "common operations picture." He explained that it would serve as the primary connection between the Department and the wider Intelligence Community as well as a primary source of information for the Department's State, local, and private sector partners. He added that I&A will be a standalone office that reports directly to him. The Secretary's testimony was otherwise short on details. For example, he left unaddressed the key issue facing both I&A and the CINT: What the focus of their intelligence analysis work should be and what value it should bring.

Congress' original plan as detailed in the Homeland Security Act of 2002 (Act) was to locate a collaborative intelligence analysis and integration center within the Department. Specifically, the Act created the Information Analysis and Infrastructure Protection Directorate (IAIP) to collect, analyze, and disseminate intelligence information about terrorist threats to the nation. In early 2003, however, just months after IAIP's creation, the Bush Administration began wresting that function from the Department by creating a separate entity under the Director of Central Intelligence: The Terrorist Threat Integration Center (TTIC). The TTIC—staffed by representatives on assignment from the CIA, the FBI, the Department, and other agencies—inherited many of the analysis responsibilities of the IAIP before IAIP even got off the ground.

The TTIC's lifespan was itself short. In order to promote effective intelligence analysis, integration and information sharing, the 9/11 Commission specifically recommended the creation of the National Counterterrorism Center (NCTC), built on the foundation of the

TTIC, to break "the mold of national government organization" by being "a center for joint operational planning and joint intelligence, staffed by personnel from the various agencies." President Bush ultimately adopted the 9/11 Commission's recommendation and directed that the TTIC be integrated into the NCTC. In response to the 9/11 Commission Report, and following the Bush Administration's creation of the NCTC by Executive Order, Congress formally established the NCTC as the primary fusion center for all terrorism intelligence analysis and integration in the Intelligence Reform and Terrorism Prevention Act in December 2004.

The NCTC's mission today largely encompasses IAIP's original analysis role. By removing the intelligence analysis and integration function from the IAIP, relocating it to the TTIC, and then finally moving it to the NCTC, the Bush Administration essentially stripped the Department of any clearly defined intelligence mission. Instead, IAIP had been relegated to matching the assessment of risks identified by the wider Intelligence Community to our nation's vulnerabilities—something it previously had not done with much success. Under the CINT's leadership, however, I&A is redefining its role and is attempting to overcome these problems of the past.

H.R. 5814 goes a long way toward addressing IAIP's shortcomings by providing a framework through which I&A can make a real contribution to the identification of terrorist threats and potential approaches to thwarting them. Specifically, the bill's various provisions are designed to: (1) promote program integration among the Department's ten separate intelligence units to drive a common intelligence mission; and (2) ensure effective information sharing with the Department's State, local, tribal, and private sector partners. The Majority and Minority have worked together on a bipartisan basis to craft the reported legislative language.

Democrats are particularly pleased with the establishment of a Homeland Security Information Sharing Fellows Program that has its genesis in the Democratic Staff's December 2005 report prepared for Representative Thompson: "Beyond Connecting the Dots: a VITAL Framework for Sharing Law Enforcement Intelligence Information." The report identified numerous security clearance, cultural, and other obstacles facing State, local, and tribal law enforcement agencies when it comes to obtaining the intelligence information they need from the Federal Government and proposed a solution based upon a highly successful approach used in the United Kingdom. This section creates a program by which State, local, and tribal law enforcement agencies can nominate officers to work alongside intelligence analysts at I&A to accomplish three key goals for improving information sharing: (1) identifying for Department intelligence analysts what kinds of homeland security information are actually of interest to law enforcement—namely, information that can be used to help thwart terrorist attacks; (2) assisting intelligence analysts in writing intelligence reports in a shareable format—provides officers with specific and actionable information without disclosing sensitive sources and methods; and (3) serving as a point of contact for officers in the field who want to share information with the Department but are unsure of where they should direct that information. This program should help

overcome the roadblocks to information sharing that continue to plague the Intelligence Community.

Additionally, the bill includes language to improve the capabilities of the Human Smuggling and Trafficking Center (HSTC) by authorizing $10 million to the Assistant Secretary of Immigration and Customs Enforcement (ICE) to provide administrative and operational support to stem human smuggling, human trafficking, and terrorism travel. The provision authorizes a sizable increase in employees and a steady funding stream to help ICE develop intelligence information in these areas that can be shared with I&A for dissemination to Federal, State, local, and tribal law enforcement and other stakeholders. The authorization should have the effect of increasing the nation's border intelligence capabilities by tracking terrorist travel and other trends at our nation's porous borders—helping policymakers move toward a more risk-based homeland security strategy that puts our money where the risks are.

OTHER PROVISIONS

As reported, H.R. 5814 includes a number of provisions originated in the Subcommittee on the Prevention of Nuclear and Biological Attack. For example, the bill authorizes the Domestic Nuclear Detection Office, the Chief Medical Officer, and the National Biosurveillance Integration System, on-going programs at the Department that are not currently authorized. It also seeks to reform the Material Threat Assessment process, the first step in Project BioShield and the main role the Department plays in the program. We appreciate that the majority incorporated language offered by Representative Langevin to specifically list the improvement of medical surge capacity as one of the duties of the Chief Medical Officer. The Committee has committed to making surge capacity a top priority, and we support this idea.

In the area of cybersecurity, the bill authorizes the position of the Assistant Secretary of Homeland Security for Cybersecurity and Telecommunications, a proposal championed by Committee Democrats for several years, and provides for new cyber security training program and equipment.

The bill also contains the key provisions of H.R. 1544, the "Faster and Smarter Funding for First Responders Act," which has previously passed the House by a wide margin.[4] These provisions will ensure that larger portions of the terrorism and law enforcement grants administered by the Department are allocated based on risk.

We are pleased that the legislation included language to address concerns by Mr. Meek about the status of the final report on a Nationwide Emergency Notification System that he included in section 7403 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458). That report, which was supposed to be completed in September 2005, would determine whether it is feasible to establish and implement an emergency telephonic alert system to notify citizens about impending emergencies. The language in this bill requires them to finish the report within 90 days of passage.

[3] H.R. 5441 was passed by the Senate on July 13, 2006.

Finally we are also pleased that the bill included Representative Bob Etheridge's (NC–2) language on the eligibility of schools for homeland funds for planning exercises.

AMENDMENTS TO H.R. 5814

The Democratic Amendment introduced by Congressman Thompson increased the bill's level of funding for the Department of Homeland Security by $6.2 billion. With competent leadership, responsible stewardship and, steady congressional oversight, these resources can be used to provide the level of security that Americans deserve.

Included in the $6.2 billion is funding for 15,000 new Border Patrol agents—more than doubling the current size of the Border Patrol, 8,000 detention beds to serve as a deterrent to illegal immigration and to end the Department's practice of "catch and release," $279 million for the Emergency Management Performance Grants program—only source of funding for State and local governments to plan and prepare for disasters, $60 million for the Metropolitan Medical Response System, which was zeroed out in the President's budget, $500 million dedicated for a grant program for the Public Safety Wireless Network, $1.9 billion for the Coast Guard's Integrated Deepwater Program, and $400 million for the port security grant program. While we certainly appreciate the Chairman's support "in spirit," we and the American people would have appreciated his vote for the amendment even more. The Thompson amendment failed on a party line vote.

Other Democratic amendments sought to more directly restructure ineffective entities within the Department. Congresswoman Loretta Sanchez (D–CA) offered an amendment to restructure, reform and reorganize the Science and Technology Directorate, which has a budget of $1.24 billion for FY 2007. The existing organizational structure established within the S&T Directorate focuses on the developers of technologies, instead of the consumers—internal components charged with securing our borders, critical infrastructure, and cyberspace. A lack of mission coordination, a complete absence of multi-year planning, a need to more effectively identify customer and mission needs are challenges that the S&T Directorate must overcome. Upon securing a commitment to explore these problems in hearings and resolve them in subsequent bipartisan legislation, Ms. Sanchez withdrew her amendment.

Representative Bill Pascrell's amendment requiring contractors with the Department of Homeland Security to attest that they have no federal tax delinquencies found favor with the Committee. The amendment was raised in response to reports by the Government Accountability Office. In a 2006 report, the Government Accountability Office (GAO) found that 10% of GSA contractors had serious federal tax problems. In their 2005 report, GAO found that there were 33,000 non-defense contractors that owed the federal government more than $3 billion in unpaid taxes. In their 2004 report, GAO found that there were 27,000 defense contractors that had failed to pay over $3 billion in taxes. The inclusion of this amendment ensures that vendors that do business with the Department of Homeland Security will be those who are not only committed to

keeping this nation secure, but those who are committed to playing by the rules.

The Priority Countermeasures Against Pathogens and Toxins amendment which was offered by Delegate Donna Christensen (VI) would have required the Secretaries of DHS and HHS to develop a strategy to achieve a dramatic reduction in the timeframe required for the delivery of drugs and vaccines to counter pathogen threats for which we have no existing countermeasures. The institution of a national rapid response "Bug-to-Drug" is needed to bolster our national biodefenses against the emerging and future threat of bioengineered biological weapons, as well as naturally occurring novel threats, such as SARS or pandemic flu. Many executive agencies, including the Department of Homeland Security, Department of Health and Human Services, Department of Defense, Department of State, Department of Agriculture, must work in collaboration to comprehensively address this problem. Dr. Christensen withdrew this amendment upon securing committee hearings on this issue.

We are pleased that Representative Lowey's amendment to streamline the Department's objective with the National Asset Database by targeting its goals, refining its organization of the collected data and upkeep of the database itself was accepted by the Committee. A recent report issued by the Department's Inspector General and recent news reports detailing the inclusion of what was termed by the Inspector General as "extremely insignificant" assets prompted this common sense amendment.

We are also pleased that the amendment offered by Representatives Markey and Sanchez, authorizing the Metropolitan Medical Response System (MMRS) grant program, was accepted by the Committee. The 124 MMRS jurisdictions across the country depend on these grants to be able to respond quickly and effectively to mass casualty events with the medical supplies needed to treat affected populations. With the threat of avian flu and other medical emergencies, MMRS remains as critical of a program today as it was at its inception in 1996 after the Oklahoma City bombing. This amendment further sends the important message that the Committee is taking its oversight role seriously when it comes to grant programs administered by the Department of Homeland Security.

Unfortunately, an amendment to protect Americans against the threat of nuclear terrorism was rejected by the Committee. Representative Langevin offered an amendment focused on the rapid deployment of radiation detection equipment at our borders to prevent the smuggling of nuclear and radiological material into our country. Funds authorized by this amendment could be used to meet a funding shortage of over 1,400 monitors related to Phase 5 of Customs and Border Protection's deployment plans for existing detection technology. Phase 5 calls for detection equipment at critical sites including the 30 highest volume international airports, major rail border crossings, and some lower volume seaports and northern border crossings. It is imperative that these sites remain impervious to illicit nuclear and radiological material. The funds could also have been used to help DNDO and Customs and Border Protection (CBP) acquire new detection technology for which the contract was just announced.

An amendment introduced by Representative Sanchez requiring rail and public transportation systems to submit security plans for review, approval, and enforcement was withdrawn upon receiving a commitment that the Committee would have a hearing focused on rail and mass transit worker security training. This amendment would have provided the Secretary with the authority to enforce the rail and public transportation security and vulnerability assessments required in the text.

An amendment offered by Representative Lowey closing loopholes and restoring the labor rights of the 42,000 Transportation Security Administration screeners failed by just one vote. This amendment would have provided screener's veterans' preference, anti-discrimination protections, retirement, whistle-blowing, and collective-bargaining rights.

Representative Markey offered an amendment directing the Transportation Security Administration (TSA) to screen air cargo over a phased-in, multi-year period. This amendment failed on a party line vote.

Representative Jackson-Lee offered several amendments related to enhancing the management of the agency. She offered an amendment that would have removed the Transportation Security Administration's exemption from the Federal Acquisition Regulation, the Competition in Contracting Act, and the Small Business Act. This exemption was initially granted with the hopes that TSA would be able to move quickly to install passenger screening equipment. Unfortunately, not only have TSA procurements been slow, they have been plagued with fraud, waste and abuse. Moreover, TSA has used its exemption from the Small Business Act to shortchange small businesses. Even according to its own statistics, the TSA is not even half way towards meeting the government-wide federal contracting goal of 23% participation of small business in agency contracting. Democrats believe that TSA's five years of contracting failures and waste is ample reason for discontinuing this exemption. Republicans, however, requested the opportunity to study this, and with the promise that the Subcommittee on Management, Integration, and Oversight would hold a hearing on the issue, Ms. Jackson-Lee withdrew her amendment. Ms. Jackson-Lee's amendment requiring federal agencies to set a goal so that at least 20 percent of the total value of contracts for response, recovery and rebuilding after a national emergency go to small, minority and disadvantaged businesses was agreed to by voice vote. Representative Jackson-Lee also offered an amendment aimed at the retention of Customs and Border Protection Agents. That amendment failed.

Mr. Markey offered an amendment, which failed 14–16, that would have provided all Department of Homeland Security employees, including employees of the Transportation Security Administration, with the same whistleblower protections Congress provided to corporate employees who are retaliated against for reporting accounting fraud in the Sarbanes-Oxley Act, and to Department of Energy and Nuclear Regulatory Commission employees and contractors in the Energy bill. Mr. Markey also offered an amendment designed to address allegations of inappropriate and potentially fraudulent use of government issued credit cards by Department

employees. This amendment, which passed the committee on a voice vote, requires the Department to create and issue guidelines and provide training to its employees on the proper use of credit cards required for official business.

Ms. Norton offered an amendment which the Committee rejected directed at eliminating the Department's personnel system. The current system, MaxHR has generated lawsuits, low employee morale and high rates of attrition. In June 2006, a federal appeals court upheld and expanded a lower court's decision that found major portions of the Department's personnel plan to be not only illegal but incapable of being implemented. This was the third time in three years that a court has told the Department that this personnel system could not go into effect.

Ms. Sanchez offered an amendment to establish limits on the amount of money that the Department of Homeland Security is authorized to reimburse under the provisions of the Intergovernmental Personnel Act, also known as "IPA." This amendment was agreed to by voice vote.

CONCLUSION

We sincerely appreciate the cooperative environment in which this legislation was produced and we are hopeful that elements of this legislation will be seriously considered by the Senate for inclusion in the FY 2008 Department of Homeland Security Authorization.

BENNIE G. THOMPSON.
ZOE LOFGREN.
BOB ETHERIDGE.
KENDRICK B. MEEK.
LORETTA SANCHEZ.
BILL PASCRELL, Jr.
JAMES LANGEVIN.
NORMAN DICKS.
JANE HARMAN.
NITA LOWEY.
DONNA M. CHRISTENSEN.
PETER DE FAZIO.
SHEILA JACKSON-LEE.
ELEANOR HOLMES NORTON.

○