109TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 109–71
Part 1

DEPARTMENT OF HOMELAND SECURITY AUTHORIZATION ACT FOR FISCAL YEAR 2006

MAY 3, 2005.—Ordered to be printed

Mr. COX, from the Committee on Homeland Security, submitted the following

R E P O R T

together with

MINORITY AND ADDITIONAL VIEWS

[To accompany H.R. 1817]

The Committee on Homeland Security, to whom was referred the bill (H.R. 1817) to authorize appropriations for fiscal year 2006 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

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Department of Homeland Security Authorization Act for Fiscal Year 2006".

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

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 2006, $34,152,143,000.

SEC. 102. BORDER PATROL AGENTS.

Of the amount authorized under section 101, there is authorized to be appropriated for fiscal year 2006 for border security and control between ports of entry, including for the hiring of 2,000 border patrol agents in addition to the number employed on the date of enactment of this Act, and related training and support costs, $1,916,427,000.

SEC. 103. DEPARTMENTAL MANAGEMENT AND OPERATIONS.

Of the amount authorized under section 101, there is authorized to be appropriated for fiscal year 2006 for departmental management and operations, $634,687,000, of which—

(1) $44,895,000 is authorized for the Department of Homeland Security Regions Initiative;

(2) $4,459,000 is authorized for Operation Integration Staff; and

(3) $56,278,000 is authorized for Office of Security initiatives.

SEC. 104. CRITICAL INFRASTRUCTURE GRANTS.

Of the amount authorized under section 101, there is authorized to be appropriated for fiscal year 2006 for grants and other assistance to improve critical infrastructure protection, $500,000,000.

SEC. 105. RESEARCH AND DEVELOPMENT.

Of the amount authorized under section 101, there are authorized to be appropriated for fiscal year 2006—

(1) $76,573,000 to support chemical countermeasure development activities of the Directorate of Science and Technology;

(2) $197,314,000 to support a nuclear detection office and related activities of such directorate;

(3) $10,000,000 for research and development of technologies capable of countering threats posed by man-portable air defense systems, including location-based technologies and noncommercial aircraft-based technologies; and

(4) $10,600,000 for the activities of such directorate conducted pursuant to subtitle G of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 441 et seq.).

SEC. 106. BORDER AND TRANSPORTATION SECURITY.

Of the amount authorized under section 101, there are authorized to be appropriated for fiscal year 2006—

(1) $826,913,000 for expenses related to Screening Coordination and Operations of the Directorate of Border and Transportation Security;

(2) $100,000,000 for weapons of mass destruction detection technology of such directorate; and

(3) $133,800,000 for the Container Security Initiative of such directorate.

SEC. 107. STATE AND LOCAL TERRORISM PREPAREDNESS.

Of the amount authorized under section 101, there is authorized to be appropriated for fiscal year 2006—

(1) $40,500,000 for the activities of the Office for Interoperability and Compatibility within the Directorate of Science and Technology pursuant to section 7303 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C 194); and

(2) $1,000,000,000 for discretionary grants for high-threat, high-density urban areas awarded by the Office of State and Local Government Coordination and Preparedness.

SEC. 108. AUTHORIZATION OF APPROPRIATIONS FOR TRAINING OF STATE AND LOCAL PERSONNEL IN BORDER STATES PERFORMING IMMIGRATION FUNCTIONS.

(a) IN GENERAL.—To carry out subsection (b), subject to such limitations as may be provided in Acts making appropriations for Management and Administration for U.S. Immigration and Customs Enforcement, there are authorized to be appropriated from such amounts $40,000,000 for fiscal year 2006, to remain available

until September 30, 2007, for the purpose of enhancing the integrity of the border security system of the United States against the threat of terrorism.

(b) USE OF FUNDS.—From amounts made available under subsection (a), the Secretary of Homeland Security may reimburse a State or political subdivision described in subsection (c) for the expenses described in subsection (d).

(c) ELIGIBLE RECIPIENTS.—A State, or a political subdivision of a State, is eligible for reimbursement under subsection (b) if the State or political subdivision—

(1) contains a location that is 30 miles or less from a border or coastline of the United States;

(2) has entered into a written agreement described in section 287(g) of the Immigration and Nationality Act (8 U.S.C. 1357(g)) under which certain officers or employees of the State or subdivision may be authorized to perform certain functions of an immigration officer; and

(3) desires such officers or employees to receive training from the Department of Homeland Security in relation to such functions.

(d) EXPENSES.—The expenses described in this subsection are actual and necessary expenses incurred by the State or political subdivision in order to permit the training described in subsection (c)(3) to take place, including expenses such as the following:

(1) Costs of travel and transportation to locations where training is provided, including mileage and related allowances for the use of a privately owned automobile.

(2) Subsistence consisting of lodging, meals, and other necessary expenses for the personal sustenance and comfort of a person required to travel away from the person's regular post of duty in order to participate in the training.

(3) A per diem allowance paid instead of actual expenses for subsistence and fees or tips to porters and stewards.

(4) Costs of securing temporary replacements for personnel traveling to, and participating in, the training.

TITLE II—TERRORISM PREVENTION, INFORMATION SHARING, AND RISK ASSESSMENT

Subtitle A—Terrorism Prevention

SEC. 201. TERRORISM PREVENTION PLAN AND RELATED BUDGET SUBMISSION.

(a) DEPARTMENT OF HOMELAND SECURITY TERRORISM PREVENTION PLAN.—

(1) REQUIREMENTS.—Not later than 1 year after the date of enactment of the Act, and on a regular basis thereafter, the Secretary of Homeland Security shall prepare and 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 Department of Homeland Security Terrorism Prevention Plan. The Plan shall be a comprehensive and integrated plan that includes the goals, objectives, milestones, and key initiatives of the Department of Homeland Security to prevent acts of terrorism on the United States, including its territories and interests.

(2) CONTENTS.—The Secretary shall include in the Plan the following elements:

(A) Identification and prioritization of groups and subgroups that pose the most significant threat of committing acts of terrorism on the United States and its interests.

(B) Identification of the most significant current, evolving, and long-term terrorist threats to the United States and its interests, including an evaluation of—

(i) the materials that may be used to carry out a potential attack;

(ii) the methods that may be used to carry out a potential attack; and

(iii) the outcome the perpetrators of acts of terrorism aim to achieve.

(C) A prioritization of the threats identified under subparagraph (B), based on an assessment of probability and consequence of such attacks.

(D) A description of processes and procedures that the Secretary shall establish to institutionalize close coordination between the Department of Homeland Security and the National Counter Terrorism Center and other appropriate United States intelligence agencies.

(E) The policies and procedures the Secretary shall establish to ensure the Department gathers real-time information from the National Counter Terrorism Center; disseminates this information throughout the Depart-

ment, as appropriate; utilizes this information to support the Department's counterterrorism responsibilities; integrates the Department's information collection and analysis functions; and disseminates this information to its operational units, as appropriate.

(F) A description of the specific actions the Secretary shall take to identify threats of terrorism on the United States and its interests, and to coordinate activities within the Department to prevent acts of terrorism, with special emphasis on prevention of terrorist access to and use of weapons of mass destruction.

(G) A description of initiatives the Secretary shall take to share critical terrorism prevention information with, and provide terrorism prevention support to, State and local governments and the private sector.

(H) A timeline, with goals and milestones, for implementing the Homeland Security Information Network, the Homeland Security Secure Data Network, and other departmental information initiatives to prevent acts of terrorism on the United States and its interests, including integration of these initiatives in the operations of the Homeland Security Operations Center.

(I) Such other terrorism prevention-related elements as the Secretary considers appropriate.

(3) CONSULTATION.—In formulating the Plan the Secretary shall consult with—

(A) the Director of National Intelligence;

(B) the Director of the National Counter Terrorism Center;

(C) the Attorney General;

(D) the Director of the Federal Bureau of Investigation;

(E) the Secretary of Defense;

(F) the Secretary of State;

(G) the Secretary of Energy;

(H) the Secretary of the Treasury; and

(I) the heads of other Federal agencies and State, county, and local law enforcement agencies as the Secretary considers appropriate.

(4) CLASSIFICATION.—The Secretary shall prepare the Plan in both classified and nonclassified forms.

(b) ANNUAL CROSSCUTTING ANALYSIS OF PROPOSED FUNDING FOR DEPARTMENT OF HOMELAND SECURITY PROGRAMS.—

(1) REQUIREMENT TO SUBMIT ANALYSIS.—The Secretary of Homeland Security shall submit to the Congress, concurrently with the submission of the President's budget for each fiscal year, a detailed, crosscutting analysis of the budget proposed for the Department of Homeland Security, by budget function, by agency, and by initiative area, identifying the requested amounts of gross and net appropriations or obligational authority and outlays for programs and activities of the Department for each of the following mission areas:

(A) To prevent terrorist attacks within the United States.

(B) To reduce the vulnerability of the United States to terrorism.

(C) To minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States.

(D) To carry out all functions of the agencies and subdivisions within the Department that are not related directly to homeland security.

(2) FUNDING ANALYSIS OF MULTIPURPOSE FUNCTIONS.—The analysis required under paragraph (1) for functions that are both related directly and not related directly to homeland security shall include a detailed allocation of funding for each specific mission area within those functions, including an allocation of funding among mission support functions, such as agency overhead, capital assets, and human capital.

(3) INCLUDED TERRORISM PREVENTION ACTIVITIES.—The analysis required under paragraph (1)(A) shall include the following activities (among others) of the Department:

(A) Collection and effective use of intelligence and law enforcement operations that screen for and target individuals who plan or intend to carry out acts of terrorism.

(B) Investigative, intelligence, and law enforcement operations that identify and disrupt plans for acts of terrorism or reduce the ability of groups or individuals to commit acts of terrorism.

(C) Investigative activities and intelligence operations to detect and prevent the introduction of weapons of mass destruction into the United States.

(D) Initiatives to detect potential, or the early stages of actual, biological, chemical, radiological, or nuclear attacks.

(E) Screening individuals against terrorist watch lists.

(F) Screening cargo to identify and segregate high-risk shipments.

(G) Specific utilization of information sharing and intelligence, both horizontally (within the Federal Government) and vertically (among Federal, State, and local governments), to detect or prevent acts of terrorism.

(H) Initiatives, including law enforcement and intelligence operations, to preempt, disrupt, and deter acts of terrorism overseas intended to strike the United States.

(I) Investments in technology, research and development, training, and communications systems that are designed to improve the performance of the Department and its agencies with respect to each of the activities listed in subparagraphs (A) through (H).

(4) SEPARATE DISPLAYS FOR MANDATORY AND DISCRETIONARY AMOUNTS.—Each analysis under paragraph (1) shall include separate displays for proposed mandatory appropriations and proposed discretionary appropriations.

SEC. 202. CONSOLIDATED BACKGROUND CHECK PROCESS.

(a) REQUIREMENT.—The Secretary shall establish a single process for conducting the security screening and background checks on individuals participating in any voluntary or mandatory departmental credentialing or registered traveler program.

(b) INCLUDED PROGRAMS.—The process established under subsection (a) shall be sufficient to meet the security requirements of all applicable Departmental programs, including—

(1) the Transportation Worker Identification Credential;

(2) the Hazmat Endorsement Credential;

(3) the Free and Secure Trade program;

(4) the NEXUS and SENTRI border crossing programs;

(5) the Registered Traveler program of the Transportation Security Administration; and

(6) any other similar program or credential considered appropriate for inclusion by the Secretary.

(c) FEATURES OF PROCESS.—The process established under subsection (a) shall include the following:

(1) A single submission of security screening information, including personal data and biometric information as appropriate, necessary to meet the security requirements of all applicable departmental programs.

(2) An ability to submit such security screening information at any location or through any process approved by the Secretary with respect to any of the applicable departmental programs.

(3) Acceptance by the Department of a security clearance issued by a Federal agency, to the extent that the security clearance process of the agency satisfies requirements that are at least as stringent as those of the applicable departmental programs under this section.

(4) Standards and procedures for protecting individual privacy, confidentiality, record retention, and addressing other concerns relating to information security.

(d) DEADLINES.—The Secretary of Homeland Security shall—

(1) submit a description of the process developed under subsection (a) to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate by not later than 6 months after the date of the enactment of this Act; and

(2) begin implementing such process by not later than 12 months after the date of the enactment of this Act.

(e) RELATIONSHIP TO OTHER LAWS.—(1) Nothing in this section affects any statutory requirement relating to the operation of the programs described in subsection (b).

(2) Nothing in this section affects any statutory requirement relating to title III of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 435b et seq.).

Subtitle B—Homeland Security Information Sharing and Analysis Enhancement

SEC. 211. SHORT TITLE.

This subtitle may be cited as the "Homeland Security Information Sharing and Analysis Enhancement Act of 2005".

SEC. 212. PROVISION OF TERRORISM-RELATED INFORMATION TO PRIVATE SECTOR OFFICIALS.

Section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is amended by adding at the end the following:

"(20) To require, in consultation with the Assistant Secretary for Infrastructure Protection, the creation and routine dissemination of analytic reports and products designed to provide timely and accurate information that has specific relevance to each of the Nation's critical infrastructure sectors (as identified in the national infrastructure protection plan issued under paragraph (5)), to private sector officials in each such sector who are responsible for protecting institutions within that sector from potential acts of terrorism and for mitigating the potential consequences of any such act.".

SEC. 213. ANALYTIC EXPERTISE ON THE THREATS FROM BIOLOGICAL AGENTS AND NUCLEAR WEAPONS.

Section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is further amended by adding at the end the following:

"(21) To ensure sufficient analytic expertise within the Office of Information Analysis to create and disseminate, on an ongoing basis, products based on the analysis of homeland security information, as defined in section 892(f)(1), with specific reference to the threat of terrorism involving the use of nuclear weapons and biological agents to inflict mass casualties or other catastrophic consequences on the population or territory of the United States.".

SEC. 214. ALTERNATIVE ANALYSIS OF HOMELAND SECURITY INFORMATION.

(a) REQUIREMENT.—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:

"SEC. 203. ALTERNATIVE ANALYSIS OF HOMELAND SECURITY INFORMATION.

"The Secretary shall establish a process and assign an individual or entity the responsibility to ensure that, as appropriate, elements of the Department conduct alternative analysis (commonly referred to as 'red-team analysis') of homeland security information, as that term is defined in section 892(f)(1), that relates to potential acts of terrorism involving the use of nuclear weapons or biological agents to inflict mass casualties or other catastrophic consequences on the population or territory of the United States.".

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

"Sec. 203. Alternative analysis of homeland security information.".

SEC. 215. ASSIGNMENT OF INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION FUNCTIONS.

Section 201(b) of the Homeland Security Act of 2002 (6 U.S.C. 121(b)) is amended by adding at the end the following:

"(4) ASSIGNMENT OF SPECIFIC FUNCTIONS.—The Under Secretary for Information Analysis and Infrastructure Protection—

"(A) shall assign to the Assistant Secretary for Information Analysis the responsibility for performing the functions described in paragraphs (1), (4), (7) through (14), (16), and (18) of subsection (d);

"(B) shall assign to the Assistant Secretary for Infrastructure Protection the responsibility for performing the functions described in paragraphs (2), (5), and (6) of subsection (d);

"(C) shall ensure that the Assistant Secretary for Information Analysis and the Assistant Secretary for Infrastructure Protection both perform the functions described in paragraphs (3), (15), (17), and (19) of subsection (d);

"(D) may assign to each such Assistant Secretary such other duties relating to such responsibilities as the Under Secretary may provide;

"(E) shall direct each such Assistant Secretary to coordinate with Federal, State, and local law enforcement agencies, and with tribal and private sector entities, as appropriate; and

"(F) shall direct the Assistant Secretary for Information Analysis to coordinate with elements of the intelligence community, as appropriate.".

SEC. 216. AUTHORITY FOR DISSEMINATING HOMELAND SECURITY INFORMATION.

(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. AUTHORITY FOR DISSEMINATING HOMELAND SECURITY INFORMATION.

"(a) PRIMARY AUTHORITY.—Except as provided in subsection (b), the Secretary shall be the executive branch official responsible for disseminating homeland secu-

rity information to State and local government and tribal officials and the private sector.

"(b) PRIOR APPROVAL REQUIRED.—No Federal official may disseminate any homeland security information, as defined in section 892(f)(1), to State, local, tribal, or private sector officials without the Secretary's prior approval, except—

"(1) in exigent circumstances under which it is essential that the information be communicated immediately; or

"(2) when such information is issued to State, local, or tribal law enforcement officials for the purpose of assisting them in any aspect of the administration of criminal justice.".

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

"Sec. 104. Authority for disseminating homeland security information.".

SEC. 217. 9/11 MEMORIAL HOMELAND SECURITY 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. 204. 9/11 MEMORIAL HOMELAND SECURITY FELLOWS PROGRAM.

"(a) ESTABLISHMENT.—

"(1) IN GENERAL.—The Secretary shall establish a fellowship program in accordance with this section for the purpose of bringing State, local, tribal, and private sector officials to participate in the work of the Homeland Security Operations Center in order to become familiar with—

"(A) the mission and capabilities of that Center; and

"(B) the role, programs, products, and personnel of the Office of Information Analysis, the Office of Infrastructure Protection, and other elements of the Department responsible for the integration, analysis, and dissemination of homeland security information, as defined in section 892(f)(1).

"(2) PROGRAM NAME.—The program under this section shall be known as the 9/11 Memorial Homeland Security Fellows Program.

"(b) ELIGIBILITY.—In order to be eligible for selection as a fellow under the program, an individual must—

"(1) have homeland security-related responsibilities; and

"(2) possess an appropriate national security clearance.

"(c) LIMITATIONS.—The Secretary—

"(1) may conduct up to 4 iterations of the program each year, each of which shall be 90 days in duration; and

"(2) shall ensure that the number of fellows selected for each iteration does not impede the activities of the Center.

"(d) CONDITION.—As a condition of selecting an individual as a fellow under the program, the Secretary shall require that the individual's employer agree to continue to pay the individual's salary and benefits during the period of the fellowship.

"(e) STIPEND.—During the period of the fellowship of an individual under the program, the Secretary shall, subject to the availability of appropriations—

"(1) provide to the individual a stipend to cover the individual's reasonable living expenses during the period of the fellowship; and

"(2) reimburse the individual for round-trip, economy fare travel to and from the individual's place of residence twice each month.".

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

"Sec. 204. 9/11 Memorial Homeland Security Fellows Program.".

SEC. 218. ACCESS TO NUCLEAR TERRORISM-RELATED INFORMATION.

Section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is further amended by adding at the end the following:

"(22) To ensure that—

"(A) the Assistant Secretary for Information Analysis receives promptly and without request all information obtained by any component of the Department if that information relates, directly or indirectly, to a threat of terrorism involving the potential use of nuclear weapons;

"(B) such information is—

"(i) integrated and analyzed comprehensively; and

"(ii) disseminated in a timely manner, including to appropriately cleared State, local, tribal, and private sector officials; and

"(C) such information is used to determine what requests the Department should submit for collection of additional information relating to that threat.".

SEC. 219. ACCESS OF ASSISTANT SECRETARY FOR INFORMATION ANALYSIS TO TERRORISM INFORMATION.

Section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is further amended by adding at the end the following:

"(23) To ensure that the Assistant Secretary for Information Analysis—

"(A) is routinely and without request given prompt access to all terrorism-related information collected by or otherwise in the possession of any component of the Department, including all homeland security information (as that term is defined in section 892(f)(1)); and

"(B) to the extent technologically feasible has direct access to all databases of any component of the Department that may contain such information.".

SEC. 220. ADMINISTRATION OF THE HOMELAND SECURITY INFORMATION NETWORK.

Section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is further amended by adding at the end the following:

"(24) To administer the homeland security information network, including—

"(A) exercising primary responsibility for establishing a secure nationwide real-time homeland security information sharing network for Federal, State, and local government agencies and authorities, tribal officials, the private sector, and other governmental and private entities involved in receiving, analyzing, and distributing information related to threats to homeland security;

"(B) ensuring that the information sharing systems, developed in connection with the network established under subparagraph (A), are utilized and are compatible with, to the greatest extent practicable, Federal, State, and local government, tribal, and private sector antiterrorism systems and protocols that have been or are being developed; and

"(C) ensuring, to the greatest extent possible, that the homeland security information network and information systems are integrated and interoperable with existing private sector technologies.".

SEC. 221. IAIP PERSONNEL RECRUITMENT.

(a) IN GENERAL.—Chapter 97 of title 5, United States Code, is amended by adding after section 9701 the following:

"§ 9702. Recruitment bonuses

"(a) IN GENERAL.—Notwithstanding any provision of chapter 57, the Secretary of Homeland Security, acting through the Under Secretary for Information Analysis and Infrastructure Protection, may pay a bonus to an individual in order to recruit such individual for a position that is primarily responsible for discharging the analytic responsibilities specified in section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) and that—

"(1) is within the Directorate for Information Analysis and Infrastructure Protection; and

"(2) would be difficult to fill in the absence of such a bonus.

In determining which individuals are to receive bonuses under this section, appropriate consideration shall be given to the Directorate's critical need for linguists.

"(b) BONUS AMOUNT, FORM, ETC.—

"(1) IN GENERAL.—The amount of a bonus under this section shall be determined under regulations of the Secretary of Homeland Security, but may not exceed 50 percent of the annual rate of basic pay of the position involved.

"(2) FORM OF PAYMENT.—A bonus under this section shall be paid in the form of a lump-sum payment and shall not be considered to be part of basic pay.

"(3) COMPUTATION RULE.—For purposes of paragraph (1), the annual rate of basic pay of a position does not include any comparability payment under section 5304 or any similar authority.

"(c) SERVICE AGREEMENTS.—Payment of a bonus under this section shall be contingent upon the employee entering into a written service agreement with the Department of Homeland Security. The agreement shall include—

"(1) the period of service the individual shall be required to complete in return for the bonus; and

"(2) the conditions under which the agreement may be terminated before the agreed-upon service period has been completed, and the effect of any such termination.

"(d) ELIGIBILITY.—A bonus under this section may not be paid to recruit an individual for—

"(1) a position to which an individual is appointed by the President, by and with the advice and consent of the Senate;

"(2) a position in the Senior Executive Service as a noncareer appointee (as defined under section 3132(a)); or

"(3) a position which has been excepted from the competitive service by reason of its confidential, policy-determining, policy-making, or policy-advocating character.

"(e) TERMINATION.—The authority to pay bonuses under this section shall terminate on September 30, 2008.

"§ 9703. Reemployed annuitants

"(a) IN GENERAL.—If an annuitant receiving an annuity from the Civil Service Retirement and Disability Fund becomes employed in a position within the Directorate for Information Analysis and Infrastructure Protection of the Department of Homeland Security, the annuitant's annuity shall continue. An annuitant so reemployed shall not be considered an employee for the purposes of chapter 83 or 84.

"(b) TERMINATION.—The exclusion pursuant to this section of the Directorate for Information Analysis and Infrastructure Protection from the reemployed annuitant provisions of chapters 83 and 84 shall terminate 3 years after the date of the enactment of this section, unless extended by the Secretary of Homeland Security. Any such extension shall be for a period of 1 year and shall be renewable.

"(c) ANNUITANT DEFINED.—For purposes of this section, the term 'annuitant' has the meaning given such term under section 8331 or 8401, whichever is appropriate.

"§ 9704. Regulations

"The Secretary of Homeland Security, in consultation with the Director of the Office of Personnel Management, may prescribe any regulations necessary to carry out section 9702 or 9703.".

(b) CLERICAL AMENDMENT.—The analysis for chapter 97 of title 5, United States Code, is amended by adding after the item relating to section 9701 the following:

"9702. Recruitment bonuses.
"9703. Reemployed annuitants.
"9704. Regulations.".

SEC. 222. INFORMATION COLLECTION REQUIREMENTS AND PRIORITIES.

(a) IN GENERAL.—Section 102 of the Homeland Security Act of 2002 (6 U.S.C. 112) is amended—

(1) by redesignating subsections (e), (f), and (g), as subsections (f), (g), and (h), respectively; and

(2) by inserting after subsection (d) the following new subsection (e):

"(e) PARTICIPATION IN FOREIGN COLLECTION REQUIREMENTS AND MANAGEMENT PROCESSES.—The Secretary shall be a member of any Federal Government interagency board, established by Executive order or any other binding interagency directive, that is responsible for establishing foreign collection information requirements and priorities for estimative analysis.".

(b) HOMELAND SECURITY INFORMATION REQUIREMENTS BOARD.—

(1) IN GENERAL.—Title I of such Act (6 U.S.C. 111 et seq.) is further amended by adding at the end the following new section:

"SEC. 105. HOMELAND SECURITY INFORMATION REQUIREMENTS BOARD.

"(a) ESTABLISHMENT OF BOARD.—There is established an interagency Homeland Security Information Requirements Board (hereinafter in this section referred to as the 'Information Requirements Board').

"(b) MEMBERSHIP.—The following officials are members of the Information Requirements Board:

"(1) The Secretary of Homeland Security, who shall serve as the Chairman of the Information Requirements Board.
"(2) The Attorney General.
"(3) The Secretary of Commerce.
"(4) The Secretary of the Treasury.
"(5) The Secretary of Defense.
"(6) The Secretary of Energy.
"(7) The Secretary of State.
"(8) The Secretary of the Interior.
"(9) The Director of National Intelligence.
"(10) The Director of the Federal Bureau of Investigation.
"(11) The Director of the National Counterterrorism Center.
"(12) The Chief Privacy Officer of the Department of Homeland Security.

"(c) FUNCTIONS.—

"(1) OVERSIGHT OF HOMELAND SECURITY REQUIREMENTS.—The Information Requirements Board shall oversee the process for establishing homeland security requirements and collection management for all terrorism-related information

and all other homeland security information (as defined in section 892(f)(1)) collected within the United States.

"(2) DETERMINATION OF COLLECTION PRIORITIES.—The Information Requirements Board shall—

"(A) determine the domestic information collection requirements for information relevant to the homeland security mission; and

"(B) prioritize the collection and use of such information.

"(3) COORDINATION OF COLLECTION REQUIREMENTS AND MANAGEMENT ACTIVITIES.—

"(A) COORDINATION WITH COUNTERPART AGENCIES.—The Chairman shall ensure that the Information Requirements Board carries out its activities in a manner that is fully coordinated with the Board's counterpart entities.

"(B) PARTICIPATION OF COUNTERPART ENTITIES.—The Chairman and the Director of National Intelligence shall ensure that each counterpart entity—

"(i) has at least one representative on the Information Requirement Board and on every subcomponent of the Board; and

"(ii) meets jointly with the Information Requirements Board (and, as appropriate, with any subcomponent of the Board) as often as the Chairman and the Director of National Intelligence determine appropriate.

"(C) COUNTERPART ENTITY DEFINED.—In this section, the term 'counterpart entity' means an entity of the Federal Government that is responsible for foreign intelligence collection requirements and management.

"(d) MEETINGS.—

"(1) IN GENERAL.—The Information Requirements Board shall meet regularly at such times and places as its Chairman may direct.

"(2) INVITED REPRESENTATIVES.—The Chairman may invite representatives of Federal agencies not specified in subsection (b) to attend meetings of the Information Requirements Board.".

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by inserting after the item relating to section 104 the following new item:

"Sec. 105. Homeland Security Information Requirements Board.".

SEC. 223. 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(d)(7) (6 U.S.C. 121(d)(7)) by inserting "under section 205" after "System"; and

(2) by adding at the end the following:

"SEC. 205. HOMELAND SECURITY ADVISORY SYSTEM.

"(a) REQUIREMENT.—The Under Secretary for Information Analysis and Infrastructure Protection 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, under the System—

"(1) shall include, in each advisory and alert regarding a threat, information on appropriate protective measures and countermeasures that may be taken in response to the threat;

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

"(3) shall not, in issuing any advisory or alert, 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 further amended by adding at the end of the items relating to subtitle A of title II the following:

"Sec. 205. Homeland Security Advisory System.".

SEC. 224. USE OF OPEN-SOURCE INFORMATION.

Section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is further amended by adding at the end the following:

"(25) To ensure that, whenever possible—

"(A) the Assistant Secretary for Information 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 Assistant Secretary for Information Analysis produces and disseminates in a classified format.".

SEC. 225. FULL AND EFFICIENT USE OF OPEN-SOURCE INFORMATION.

(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. 206. FULL AND EFFICIENT USE OF OPEN-SOURCE INFORMATION.

"The Under Secretary shall ensure that, in meeting their analytic responsibilities under section 201(d) and in formulating requirements for collection of additional information, the Assistant Secretary for Information Analysis and the Assistant Secretary for Infrastructure Protection make full and efficient use of open-source information wherever possible.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by inserting after the item relating to section 205 the following:

"Sec. 206. Full and efficient use of open-source information.".

TITLE III—DOMESTIC PREPAREDNESS AND PROTECTION

Subtitle A—Preparedness and Protection

SEC. 301. NATIONAL TERRORISM EXERCISE PROGRAM.

(a) IN GENERAL.—Section 430(c) of the Homeland Security Act of 2002 (6 U.S.C. 238) is amended by striking "and" after the semicolon at the end of paragraph (8), by striking the period at the end of paragraph (9) and inserting "; and", and by adding at the end the following:

"(10) designing, developing, performing, and evaluating exercises at the national, State, territorial, regional, local, and tribal levels of government that incorporate government officials, emergency response providers, public safety agencies, the private sector, international governments and organizations, and other appropriate entities to test the Nation's capability to prevent, prepare for, respond to, and recover from threatened or actual acts of terrorism.".

(b) NATIONAL TERRORISM EXERCISE PROGRAM.—

(1) ESTABLISHMENT OF PROGRAM.—Title VIII of the Homeland Security Act of 2002 (Public Law 107–296) is amended by adding at the end the following new subtitle:

"Subtitle J—Terrorism Preparedness Exercises

"SEC. 899a. NATIONAL TERRORISM EXERCISE PROGRAM.

"(a) IN GENERAL.—The Secretary, through the Office for Domestic Preparedness, shall establish a National Terrorism Exercise Program for the purpose of testing and evaluating the Nation's capabilities to prevent, prepare for, respond to, and recover from threatened or actual acts of terrorism that—

"(1) enhances coordination for terrorism preparedness between all levels of government, emergency response providers, international governments and organizations, and the private sector;

"(2) is—

"(A) multidisciplinary in nature, including, as appropriate, information analysis and cybersecurity components;

"(B) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;

"(C) carried out with the minimum degree of notice to involved parties regarding the timing and details of such exercises, consistent with safety considerations;

"(D) evaluated against performance measures and followed by corrective action to solve identified deficiencies; and

"(E) assessed to learn best practices, which shall be shared with appropriate Federal, State, territorial, regional, local, and tribal personnel, authorities, and training institutions for emergency response providers; and

"(3) assists State, territorial, local, and tribal governments with the design, implementation, and evaluation of exercises that—

"(A) conform to the requirements of paragraph (2); and

"(B) are consistent with any applicable State homeland security strategy or plan.

"(b) NATIONAL LEVEL EXERCISES.—The Secretary, through the National Terrorism Exercise Program, shall perform on a periodic basis national terrorism preparedness exercises for the purposes of—

"(1) involving top officials from Federal, State, territorial, local, tribal, and international governments, as the Secretary considers appropriate;

"(2) testing and evaluating the Nation's capability to detect, disrupt, and prevent threatened or actual catastrophic acts of terrorism, especially those involving weapons of mass destruction; and

"(3) testing and evaluating the Nation's readiness to respond to and recover from catastrophic acts of terrorism, especially those involving weapons of mass destruction.

"(c) CONSULTATION WITH FIRST RESPONDERS.—In implementing the responsibilities described in subsections (a) and (b), the Secretary shall consult with a geographic (including urban and rural) and substantive cross section of governmental and nongovernmental first responder disciplines, including as appropriate—

"(1) Federal, State, and local first responder training institutions;

"(2) representatives of emergency response providers; and

"(3) State and local officials with an expertise in terrorism preparedness.".

(2) 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 title VIII the following:

"Subtitle J—Terrorism Preparedness Exercises

"Sec. 899a. National terrorism exercise program.".

(c) TOPOFF PREVENTION EXERCISE.—No later than one year after the date of enactment of this Act, the Secretary of Homeland Security shall design and carry out a national terrorism prevention exercise for the purposes of—

(1) involving top officials from Federal, State, territorial, local, tribal, and international governments; and

(2) testing and evaluating the Nation's capability to detect, disrupt, and prevent threatened or actual catastrophic acts of terrorism, especially those involving weapons of mass destruction.

SEC. 302. TECHNOLOGY DEVELOPMENT AND TRANSFER.

(a) ESTABLISHMENT OF TECHNOLOGY CLEARINGHOUSE.—Not later than 90 days after the date of enactment of this Act, the Secretary shall complete the establishment of the Technology Clearinghouse under section 313 of the Homeland Security Act of 2002.

(b) TRANSFER PROGRAM.—Section 313 of the Homeland Security Act of 2002 (6 U.S.C. 193) is amended—

(1) by adding at the end of subsection (b) the following new paragraph:

"(6) The establishment of a homeland security technology transfer program to facilitate the identification, modification, and commercialization of technology and equipment for use by Federal, State, and local governmental agencies, emergency response providers, and the private sector to prevent, prepare for, or respond to acts of terrorism.";

(2) by redesignating subsection (c) as subsection (d); and

(3) by inserting after subsection (b) the following new subsection:

"(c) TECHNOLOGY TRANSFER PROGRAM.—In developing the program described in subsection (b)(6), the Secretary, acting through the Under Secretary for Science and Technology, shall—

"(1) in consultation with the other Under Secretaries of the Department and the Director of the Office for Domestic Preparedness, on an ongoing basis—

"(A) conduct surveys and reviews of available appropriate technologies that have been, or are in the process of being developed, tested, evaluated, or demonstrated by the Department, other Federal agencies, or the private sector or foreign governments and international organizations and that may be useful in assisting Federal, State, and local governmental agencies, emergency response providers, or the private sector to prevent, prepare for, or respond to acts of terrorism;

"(B) conduct or support research, development, tests, and evaluations, as appropriate of technologies identified under subparagraph (A), including any necessary modifications to such technologies for antiterrorism use;

"(C) communicate to Federal, State, and local governmental agencies, emergency response providers, or the private sector the availability of such technologies for antiterrorism use, as well as the technology's specifications,

satisfaction of appropriate standards, and the appropriate grants available from the Department to purchase such technologies;

"(D) coordinate the selection and administration of all technology transfer activities of the Science and Technology Directorate, including projects and grants awarded to the private sector and academia; and

"(E) identify priorities based on current risk assessments within the Department of Homeland Security for identifying, researching, developing, testing, evaluating, modifying, and fielding existing technologies for antiterrorism purposes;

"(2) in support of the activities described in paragraph (1)—

"(A) consult with Federal, State, and local emergency response providers;

"(B) consult with government agencies and nationally recognized standards development organizations as appropriate;

"(C) enter into agreements and coordinate with other Federal agencies, foreign governments, and national and international organizations as the Secretary determines appropriate, in order to maximize the effectiveness of such technologies or to facilitate commercialization of such technologies; and

"(D) consult with existing technology transfer programs and Federal and State training centers that research, develop, test, evaluate, and transfer military and other technologies for use by emergency response providers; and

"(3) establish a working group in coordination with the Secretary of Defense to advise and assist the technology clearinghouse in the identification of military technologies that are in the process of being developed, or are developed, by the Department of Defense or the private sector, which may include—

"(A) representatives from the Department of Defense or retired military officers;

"(B) nongovernmental organizations or private companies that are engaged in the research, development, testing, or evaluation of related technologies or that have demonstrated prior experience and success in searching for and identifying technologies for Federal agencies;

"(C) Federal, State, and local emergency response providers; and

"(D) to the extent the Secretary considers appropriate, other organizations, other interested Federal, State, and local agencies, and other interested persons.".

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the Under Secretary for Science and Technology shall transmit to the Congress a description of the progress the Department has made in implementing the provisions of section 313 of the Homeland Security Act of 2002, as amended by this Act, including a description of the process used to review unsolicited proposals received as described in subsection (b)(3) of such section.

(d) SAVINGS CLAUSE.—Nothing in this section (including the amendments made by this section) shall be construed to alter or diminish the effect of the limitation on the authority of the Secretary of Homeland Security under section 302(4) of the Homeland Security Act of 2002 (6 U.S.C. 182(4)) with respect to human health-related research and development activities.

SEC. 303. REVIEW OF ANTITERRORISM ACQUISITIONS.

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

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

(2) assess whether such product, equipment, service (including support services), device, or technology is an appropriate candidate for the litigation and risk management protections of subtitle G of title VIII of the Homeland Security Act of 2002.

(b) SUMMARY AND CLASSIFICATION REPORT.—Not later than 180 days after the date of enactment of this Act, the Secretary shall transmit to the Congress a report—

(1) describing each product, equipment, service (including support services), device, and technology identified under subsection (a) that the Secretary believes would be an appropriate candidate for the litigation and risk management protections of subtitle G of title VIII of the Homeland Security Act of 2002;

(2) listing each such product, equipment, service (including support services), device, and technology in order of priority for deployment in accordance with current terrorism risk assessment information; and

(3) setting forth specific actions taken, or to be taken, to encourage or require persons or entities that sell or otherwise provide such products, equipment, services (including support services), devices, and technologies to apply for the litigation and risk management protections of subtitle G of title VIII of the Homeland Security Act of 2002, and to ensure prioritization of the Department's review of such products, equipment, services, devices, and technologies under such Act in accordance with the prioritization set forth in paragraph (2) of this subsection.

SEC. 304. CENTER OF EXCELLENCE FOR BORDER SECURITY.

The Secretary of Homeland Security shall establish a university-based Center for Excellence for Border Security following the merit-review processes and procedures that have been established for selecting University Programs Centers of Excellence. The Center shall prioritize its activities on the basis of risk to address the most significant threats, vulnerabilities, and consequences posed by the Nation's borders and border control systems, including the conduct of research, the examination of existing and emerging border security technology and systems, and the provision of education, technical, and analytical assistance for the Department of Homeland Security to effectively secure the Nation's borders.

SEC. 305. REQUIREMENTS RELATING TO THE CONTAINER SECURITY INITIATIVE (CSI).

(a) RISK ASSESSMENT AND DESIGNATION OF NEW FOREIGN SEAPORTS.—

(1) RISK ASSESSMENT.—The Secretary of Homeland Security shall conduct a risk assessment of each foreign seaport that the Secretary is considering designating as a port under the Container Security Initiative (CSI) on or after the date of the enactment of this Act. Each such assessment shall evaluate the level of risk for the potential compromise of cargo containers by terrorists or terrorist weapons.

(2) DESIGNATION.—The Secretary is authorized to designate a foreign seaport as a port under CSI on or after the date of the enactment of this Act only if the Secretary determines, based on a risk assessment under paragraph (1) and a cost-benefit analysis, that the benefits of designating such port outweigh the cost of expanding the program to such port.

(b) DEPLOYMENT OF INSPECTION EQUIPMENT TO NEW CSI PORTS.—

(1) DEPLOYMENT.—The Secretary is authorized to assist in the loaning of nonintrusive inspection equipment for cargo containers, on a nonreimbursable basis, at each CSI port designated under subsection (a)(2) and provide training for personnel at the CSI port to operate the nonintrusive inspection equipment.

(2) ADDITIONAL REQUIREMENTS.—The Secretary shall establish technical capability requirements and standard operating procedures for nonintrusive inspection equipment described in paragraph (1) and shall require each CSI port to agree to operate such equipment in accordance with such requirements and procedures as a condition for receiving the equipment and training under such paragraph.

(c) DEPLOYMENT OF PERSONNEL TO NEW CSI PORTS; REEVALUATION OF PERSONNEL AT ALL CSI PORTS.—

(1) DEPLOYMENT.—The Secretary shall deploy Department of Homeland Security personnel to each CSI port designated under subsection (a)(1) with respect to which the Secretary determines that the deployment is necessary to successfully implement the requirements of CSI at the port.

(2) REEVALUATION.—The Secretary shall periodically review relevant risk assessment information with respect to all CSI ports at which Department of Homeland Security personnel are deployed to assess whether or not continued deployment of such personnel, in whole or in part, is necessary to successfully implement the requirements of CSI at the port.

(d) INSPECTION AND SCREENING AT UNITED STATES PORTS OF ENTRY.—Cargo containers arriving at a United States port of entry from a CSI port shall undergo the same level of inspection and screening for potential compromise by terrorists or terrorist weapons as cargo containers arriving at a United States port of entry from a foreign seaport that is not participating in CSI unless the containers were initially inspected at the CSI port at the request of CSI personnel and such personnel verify and electronically record that the inspection indicates that the containers have not been compromised by terrorists or terrorist weapons.

(e) DEFINITION.—In this section, the term "Container Security Initiative" or "CSI" means the program carried out by the Department of Homeland Security under which the Department enters into agreements with foreign seaports to—

(1) establish security criteria to identify high-risk maritime cargo containers bound for the United States based on advance information; and

(2) screen or inspect such maritime cargo containers for potential compromise by terrorists or terrorist weapons prior to shipment to the United States.

SEC. 306. SECURITY OF MARITIME CARGO CONTAINERS.

(a) REGULATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall issue regulations for the security of maritime cargo containers moving within the intermodal transportation system in accordance with the requirements of paragraph (2).

(2) REQUIREMENTS.—The regulations issued pursuant to paragraph (1) shall be in accordance with recommendations of the Maritime Transportation Security Act Subcommittee of the Advisory Committee on Commercial Operations of the Department of Homeland Security, including recommendations relating to obligation to seal, recording of seal changes, modal changes, seal placement, ocean carrier seal verification, and addressing seal anomalies.

(b) INTERNATIONAL AGREEMENTS.—The Secretary shall seek to enter into agreements with foreign countries and international organizations to establish standards for the security of maritime cargo containers moving within the intermodal transportation system that, to the maximum extent practicable, meet the requirements of subsection (a)(2).

(c) CONTAINER TARGETING STRATEGY.—

(1) STRATEGY.—The Secretary shall develop a strategy to improve the ability of the Department of Homeland Security to use information contained in shipping bills of lading to identify and provide additional review of anomalies in such bills of lading. The strategy shall include a method of contacting shippers in a timely fashion to verify or explain any anomalies in shipping bills of lading.

(2) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees a report on the implementation of this subsection, including information on any data searching technologies that will be used to implement the strategy.

(d) CONTAINER SECURITY DEMONSTRATION PROGRAM.—

(1) PROGRAM.—The Secretary is authorized to establish and carry out a demonstration program that integrates nonintrusive inspection equipment, including radiation detection equipment and gamma ray inspection equipment, at an appropriate United States seaport, as determined by the Secretary.

(2) REQUIREMENT.—The demonstration program shall also evaluate automatic identification methods for containers and vehicles and a data sharing network capable of transmitting inspection data between ports and appropriate entities within the Department of Homeland Security.

(3) REPORT.—Upon completion of the demonstration program, the Secretary shall submit to the appropriate congressional committees a report on the implementation of this subsection.

(e) CONSOLIDATION OF CONTAINER SECURITY PROGRAMS.—The Secretary shall consolidate all programs of the Department of Homeland Security relating to the security of maritime cargo containers, including the demonstration program established pursuant to subsection (d), to achieve enhanced coordination and efficiency.

SEC. 307. SECURITY PLAN FOR GENERAL AVIATION AT RONALD REAGAN WASHINGTON NATIONAL AIRPORT.

Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security shall implement section 823(a) of the Vision 100—Century of Aviation Reauthorization Act (49 U.S.C. 41718 note; 117 Stat. 2595).

SEC. 308. INTEROPERABLE COMMUNICATIONS ASSISTANCE.

(a) FINDINGS.—The Congress finds the following:

(1) The 9/11 Commission determined that the inability of first responders to communicate effectively on September 11, 2001 was a critical obstacle to an effective multi-jurisdictional response.

(2) Many jurisdictions across the country still experience difficulties communicating that may contribute to confusion, delays, or added risks when responding to an emergency.

(3) During fiscal year 2004, the Office for Domestic Preparedness awarded over $834,000,000 for 2,912 projects through Department of Homeland Security grant programs for the purposes of improving communications interoperability.

(4) Interoperable communications systems are most effective when designed to comprehensively address, on a regional basis, the communications of all types of public safety agencies, first responder disciplines, and State and local government facilities.

(5) Achieving communications interoperability is complex due to the extensive training, system modifications, and agreements among the different jurisdictions that are necessary to implement effective communications systems.

(6) The Congress authorized the Department of Homeland Security to create an Office for Interoperability and Compatibility in the Intelligence Reform and Terrorism Prevention Act of 2004 to, among other things, establish a comprehensive national approach, coordinate federal activities, accelerate the adoption of standards, and encourage research and development to achieve interoperable communications for first responders.

(7) The Office for Interoperability and Compatibility includes the SAFECOM Program that serves as the umbrella program within the Federal government to improve public safety communications interoperability, and has developed the RAPIDCOM program, the Statewide Communications Interoperability Planning Methodology, and a Statement of Requirements to provide technical, planning, and purchasing assistance for Federal departments and agencies, State and local governments, and first responders.

(b) SENSE OF CONGRESS.—It is the sense of the Congress that the Department of Homeland Security should implement as expeditiously as possible the initiatives assigned to the Office for Interoperability and Compatibility under section 7303 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194), including specifically the following:

(1) Establishing a comprehensive national approach to achieving public safety interoperable communications.

(2) Issuing letters of intent to commit future funds for jurisdictions through existing homeland security grant programs to applicants as appropriate to encourage long-term investments that may significantly improve communications interoperability.

(3) Providing technical assistance to additional urban and other high-risk areas to support the establishment of consistent, secure, and effective interoperable communications capabilities.

(4) Completing the report to the Congress on the Department's plans for accelerating the development of national voluntary consensus standards for public safety interoperable communications, a schedule of milestones for such development, and achievements of such development, by no later than 30 days after the date of enactment of this Act.

SEC. 309. REPORT TO CONGRESS ON IMPLEMENTATION OF RECOMMENDATIONS REGARDING PROTECTION OF AGRICULTURE.

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 by no later than 120 days after the date of the enactment of this Act regarding how the Department of Homeland Security will implement the applicable recommendations from the Government Accountability Office report entitled "Homeland Security: Much is Being Done to Protect Agriculture from a Terrorist Attack, but Important Challenges Remain" (GAO–05–214).

Subtitle B—Department of Homeland Security Cybersecurity Enhancement

SEC. 311. SHORT TITLE.

This subtitle may be cited as the "Department of Homeland Security Cybersecurity Enhancement Act of 2005".

SEC. 312. ASSISTANT SECRETARY FOR CYBERSECURITY.

(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. ASSISTANT SECRETARY FOR CYBERSECURITY.

"(a) IN GENERAL.—There shall be in the Directorate for Information Analysis and Infrastructure Protection a National Cybersecurity Office headed by an Assistant Secretary for Cybersecurity (in this section referred to as the 'Assistant Secretary'), who shall assist the Secretary in promoting cybersecurity for the Nation.

"(b) GENERAL AUTHORITY.—The Assistant Secretary, subject to the direction and control of the Secretary, shall have primary authority within the Department for all cybersecurity-related critical infrastructure protection programs of the Department, including with respect to policy formulation and program management.

"(c) RESPONSIBILITIES.—The responsibilities of the Assistant Secretary 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; and

"(ii) aid in the detection and warning of attacks on, and in the restoration of, cybersecurity infrastructure in the aftermath of such attacks;

"(B) a national cybersecurity threat and vulnerability reduction program that identifies cybersecurity vulnerabilities that would have a national effect on critical infrastructure, performs vulnerability assessments on information technologies, and coordinates the mitigation of such vulnerabilities;

"(C) a national cybersecurity awareness and training program that promotes cybersecurity awareness among the public and the private sectors and promotes cybersecurity training and education programs;

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

"(E) a national security and international cybersecurity cooperation program to help foster Federal efforts to enhance international cybersecurity awareness and cooperation.

"(2) To coordinate with 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 other directorates and offices within the Department on the cybersecurity aspects of their missions.

"(4) To coordinate with the Under Secretary for Emergency Preparedness and Response to ensure that the National Response Plan developed pursuant to section 502(6) of the Homeland Security Act of 2002 (6 U.S.C. 312(6)) includes appropriate measures for the recovery of the cybersecurity elements of critical infrastructure.

"(5) To develop processes for information sharing with the private sector, consistent with section 214, that—

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

"(B) consider roles of Federal, State, local, and foreign governments and the private sector, including the insurance industry and auditors.

"(6) 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.

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

"(8) To consult with the Office for Domestic Preparedness to ensure that realistic cybersecurity scenarios are incorporated into tabletop and recovery exercises.

"(9) To consult and coordinate, as appropriate, with other Federal agencies on cybersecurity-related programs, policies, and operations.

"(10) To consult and coordinate within the Department and, where appropriate, with other relevant Federal agencies, on security of digital control systems, such as Supervisory Control and Data Acquisition (SCADA) systems.

"(d) AUTHORITY OVER THE NATIONAL COMMUNICATIONS SYSTEM.—The Assistant Secretary shall have primary authority within the Department over the National Communications System.".

(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 A of title II the following:

"Sec. 207. Assistant Secretary for Cybersecurity.".

SEC. 313. CYBERSECURITY DEFINED.

Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) is amended by adding at the end the following:

"(17)(A) The term 'cybersecurity' means the prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

"(B) In this paragraph—

"(i) each of the terms 'damage' and 'computer' has the meaning that term has in section 1030 of title 18, United States Code; and

"(ii) each of the terms 'electronic communications system', 'electronic communication service', 'wire communication', and 'electronic communication' has the meaning that term has in section 2510 of title 18, United States Code.".

SEC. 314. CYBERSECURITY TRAINING PROGRAMS AND EQUIPMENT.

(a) IN GENERAL.—The Secretary of Homeland Security, acting through the Assistant Secretary for Cybersecurity, 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, acting through the Assistant Secretary for Cybersecurity 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 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 under section 101, there is authorized to be appropriated to the Secretary for carrying out this section $3,700,000 for fiscal year 2006.

(e) DEFINITIONS.—In 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. 315. INFORMATION SECURITY REQUIREMENTS AND OMB RESPONSIBILITIES NOT AFFECTED.

(a) IN GENERAL.—This subtitle does not affect—

(1) any information security requirement under any other Federal law; or

(2) the responsibilities of the Director of the Office of Management and Budget under any other Federal law.

(b) LAWS INCLUDED.—The laws referred to in subsection (a) include the following:

(1) Chapter 35 of title 44, United States Code, popularly known as the Paperwork Reduction Act.

(2) The Clinger-Cohen Act of 1996 (divisions D and E of Public Law 104–106), including the provisions of law enacted by amendments made by that Act.

(3) The Federal Information Security Management Act of 2002 (title III of Public Law 107–347), including the provisions of law enacted by amendments made by that Act.

Subtitle C—Security of Public Transportation Systems

SEC. 321. SECURITY BEST PRACTICES.

Not later than 120 days after the date of enactment of this Act, the Secretary of Homeland Security shall develop, disseminate to appropriate owners, operators, and providers of public transportation systems, public transportation employees and employee representatives, and Federal, State, and local officials, and transmit to Congress, a report containing best practices for the security of public transportation systems. In developing best practices, the Secretary shall be responsible for consulting with and collecting input from owners, operators, and providers of public transportation systems, public transportation employee representatives, first responders, industry associations, private sector experts, academic experts, and appropriate Federal, State, and local officials.

SEC. 322. PUBLIC AWARENESS.

Not later than 90 days after the date of enactment of this Act, the Secretary of Homeland Security shall develop a national plan for public outreach and awareness. Such plan shall be designed to increase awareness of measures that the general public, public transportation passengers, and public transportation employees can take to increase public transportation system security. Such plan shall also provide outreach to owners, operators, providers, and employees of public transportation systems to improve their awareness of available technologies, ongoing research and development efforts, and available Federal funding sources to improve public transportation security. Not later than 9 months after the date of enactment of this Act, the Secretary shall implement the plan developed under this section.

Subtitle D—Critical Infrastructure Prioritization

SEC. 331. CRITICAL INFRASTRUCTURE.

(a) COMPLETION OF PRIORITIZATION.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall complete the prioritization of the Nation's critical infrastructure according to all of the following criteria:

(1) The threat of terrorist attack, based on threat information received and analyzed by the Office of Information Analysis of the Department regarding the intentions and capabilities of terrorist groups and other potential threats to the Nation's critical infrastructure.

(2) The likelihood that an attack would cause the destruction or significant disruption of such infrastructure.

(3) The likelihood that an attack would result in substantial numbers of deaths and serious bodily injuries, a substantial adverse impact on the national economy, or a substantial adverse impact on national security.

(b) COOPERATION.—Such prioritization shall be developed in cooperation with other relevant Federal agencies, State, local, and tribal governments, and the private sector, as appropriate.

SEC. 332. SECURITY REVIEW.

(a) REQUIREMENT.—Not later than 9 months after the date of the enactment of this Act, the Secretary, in coordination with other relevant Federal agencies, State, local, and tribal governments, and the private sector, as appropriate, shall—

(1) review existing Federal, State, local, tribal, and private sector plans for securing the critical infrastructure included in the prioritization developed under section 331;

(2) recommend changes to existing plans for securing such infrastructure, as the Secretary determines necessary; and

(3) coordinate and contribute to protective efforts of other Federal, State, local, and tribal agencies and the private sector, as appropriate, as directed in Homeland Security Presidential Directive 7.

(b) CONTENTS OF PLANS.—The recommendations made under subsection (a)(2) shall include—

(1) necessary protective measures to secure such infrastructure, including milestones and timeframes for implementation; and

(2) to the extent practicable, performance metrics to evaluate the benefits to both national security and the Nation's economy from the implementation of such protective measures.

SEC. 333. IMPLEMENTATION REPORT.

(a) IN GENERAL.—Not later than 15 months after the date of the enactment of this Act, the Secretary shall submit a 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 implementation of section 332. Such report shall detail—

(1) the Secretary's review and coordination of security plans under section 332; and

(2) the Secretary's oversight of the execution and effectiveness of such plans.

(b) UPDATE.—Not later than 1 year after the submission of the report under subsection (a), the Secretary shall provide an update of such report to the congressional committees described in subsection (a).

SEC. 334. PROTECTION OF INFORMATION.

Information that is generated, compiled, or disseminated by the Department of Homeland Security in carrying out this section—

(1) is exempt from disclosure under section 552 of title 5, United States Code; and

(2) shall not, if provided by the Department to a State or local government or government agency—

(A) be made available pursuant to any State or local law requiring disclosure of information or records;

(B) otherwise be disclosed or distributed to any person by such State or local government or government agency without the written consent of the Secretary; or

(C) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act.

TITLE IV—MISCELLANEOUS

SEC. 401. BORDER SECURITY AND ENFORCEMENT COORDINATION AND OPERATIONS.

(a) FINDINGS.—The Congress makes the following findings:

(1) In creating the Department of Homeland Security, the Congress sought to enhance the Nation's capabilities to prevent, protect against, and respond to terrorist acts by consolidating existing Federal agencies with homeland security functions into a single new Department, and by realigning the missions of those legacy agencies to more directly support our national homeland security efforts.

(2) As part of this massive government reorganization, section 442 of the Homeland Security Act of 2002 (Public Law 107–273) established a Bureau of Border Security and transferred into it all of the functions, programs, personnel, assets, and liabilities pertaining to the following programs: the Border Patrol; alien detention and removal; immigration-related intelligence, investigations, and enforcement activities; and immigration inspections at ports of entry.

(3) Title IV of the Homeland Security Act of 2002 (Public Law 107–273) also transferred to the new Department the United States Customs Service, as a distinct entity within the new Department, to further the Department's border integrity mission.

(4) Utilizing its reorganization authority provided in the Homeland Security Act of 2002, the President submitted a reorganization plan for the Department on January 30, 2003.

(5) This plan merged the customs and immigration border inspection and patrol functions, along with agricultural inspections functions, into a new entity called United States Customs and Border Protection.

(6) The plan also combined the customs and immigration enforcement agents, as well as the Office of Detention and Removal Operations, the Office of Federal Protective Service, the Office of Federal Air Marshal Service, and the Office of Intelligence, into another new entity called United States Immigration and Customs Enforcement.

(7) The President's January 30, 2003, reorganization plan did not explain the reasons for separating immigration inspection and border patrol functions from other immigration-related enforcement activities, which was contrary to the single Bureau of Border Security as prescribed by the Congress in the section 441 of the Homeland Security Act of 2002.

(8) Two years after this structure has been in effect, questions remain about whether the Department has organized itself properly, and is managing its customs and immigration enforcement and border security resources in the most efficient, sensible, and effective manner.

(9) The current structure has resulted in less cooperation and information sharing between these two critical functions than is desirable, and has caused operational and administrative difficulties that are hampering efforts to secure our borders and ensure the integrity of our border control system.

(10) United States Immigration and Customs Enforcement has faced major budgetary challenges that are, in part, attributable to the inexact division of resources upon the separation of immigration functions. These budget shortfalls have forced United States Immigration and Customs Enforcement to impose hiring freezes and to release aliens that otherwise should be detained.

(11) The current structure also has resulted in unnecessary overlap and duplication between United States Immigration and Customs Enforcement and United States Customs and Border Protection, both in the field and at the headquarters level. There are intelligence, legislative affairs, public affairs, and international affairs offices in both agencies.

(12) Border security and customs and immigration enforcement should be one seamless mission.

(b) REPORT.—

(1) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act, the Secretary of Homeland Security shall review and evaluate the current organizational structure of the Department of Homeland Security established by the President's January 30, 2003, reorganization plan and submit a report of findings and recommendations to the Congress.

(2) CONTENTS OF REPORT.—The report shall include—

(A) a description of the rationale for, and any benefits of, the current organizational division of United States Immigration and Customs Enforcement and United States Customs and Border Protection, with respect to the Department's immigration and customs missions;

(B) a description of the organization, missions, operations, and policies of United States Customs and Border Protection and United States Immigration and Customs Enforcement, and areas of unnecessary overlap or operational gaps among and between these missions;

(C) an analysis of alternative organizational structures that could provide a more effective way to deliver maximum efficiencies and mission success;

(D) a description of the current role of the Directorate of Border and Transportation Security with respect to providing adequate direction and oversight of the two agencies, and whether this management structure is still necessary;

(E) an analysis of whether the Federal Air Marshals and the Federal Protective Service are properly located within the Department within United States Immigration and Customs Enforcement;

(F) the proper placement and functions of a specialized investigative and patrol unit operating at the southwest border on the Tohono O'odham Nation, known as the Shadow Wolves;

(G) the potential costs of reorganization, including financial, programmatic, and other costs, to the Department; and

(H) recommendations for correcting the operational and administrative problems that have been caused by the division of United States Customs and Border Protection and United States Immigration and Customs Enforcement, including any appropriate reorganization plans.

SEC. 402. GAO REPORT TO CONGRESS.

Not later than 6 months after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Congress a report that sets forth—

(1) an assessment of the effectiveness of the organizational and management structure of the Department of Homeland Security in meeting the Department's missions; and

(2) recommendations to facilitate and improve the organization and management of the Department to best meet those missions.

SEC. 403. PLAN FOR ESTABLISHING CONSOLIDATED AND COLOCATED REGIONAL OFFICES.

Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall develop and submit to the Congress a plan for establishing consolidated and colocated regional offices for the Department of Homeland Security in accordance with section 706 of the Homeland Security Act of 2002 (6 U.S.C. 346).

SEC. 404. PLAN TO REDUCE WAIT TIMES.

Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security shall develop a plan—

(1) to improve the operational efficiency of security screening checkpoints at commercial service airports so that average peak waiting periods at such checkpoints do not exceed 20 minutes; and

(2) to ensure that there are no significant disparities in immigration and customs processing times among airports that serve as international gateways.

SEC. 405. DENIAL OF TRANSPORTATION SECURITY CARD.

Section 70105(c) of title 46, United States Code, is amended—

(1) in paragraph (3) by inserting before the period "before an administrative law judge"; and

(2) by adding at the end the following:

"(5) In making a determination under paragraph (1)(D), the Secretary shall not consider a felony conviction if—

"(A) that felony occurred more than 7 years prior to the date of the Secretary's determination; and

"(B) the felony was not related to terrorism (as that term is defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)).".

SEC. 406. TRANSFER OF EXISTING CUSTOMS PATROL OFFICERS UNIT AND ESTABLISHMENT OF NEW CPO UNITS IN THE BUREAU OF IMMIGRATION AND CUSTOMS ENFORCEMENT.

(a) TRANSFER OF EXISTING UNIT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall transfer to the Bureau of Immigration and Customs Enforcement all functions (including the personnel, assets, and obligations held by or available in connection with such functions) of the Customs Patrol Officers unit of the Bureau of Customs and Border Protection operating on the Tohono O'odham Indian reservation (commonly known as the 'Shadow Wolves' unit).

(b) ESTABLISHMENT OF NEW UNITS.—The Secretary is authorized to establish within the Bureau of Immigration and Customs Enforcement additional units of Customs Patrol Officers in accordance with this section.

(c) DUTIES.—The Secretary is authorized to establish within the Bureau of Immigration and Customs Enforcement additional units of Customs Patrol Officers in accordance with this section.

(d) BASIC PAY FOR JOURNEYMAN OFFICERS.—The rate of basic pay for a journeyman Customs Patrol Officer in a unit described in this section shall be not less than the rate of basic pay for GS–13 of the General Schedule.

(e) SUPERVISORS.—Each unit described under this section shall be supervised by a Chief Customs Patrol Officer, who shall have the same rank as a resident agent-in-charge of the Office of Investigations.

PURPOSE AND SUMMARY

The purpose of H.R. 1817 is To authorize appropriations for fiscal year 2006 for the Department of Homeland Security, and for other purposes.

BACKGROUND AND NEED FOR LEGISLATION

The core mission of the Department of Homeland Security (DHS) is threefold: first, preventing terrorist attacks within the United States; second, reducing America's vulnerability to terrorism; and third, responding to and recovering from terrorist attacks if and when they occur. It is equally essential that the Department carry out this mission in a manner that promotes our Nation's economic security through the facilitation of legitimate trade and travel. The President's proposed discretionary budget for the Department—and its 180,000 employees—for Fiscal Year 2006 is $34.2 billion. With mandatory funding accounts included, the total exceeds $41 billion. DHS is thus the third largest Cabinet agency, and its challenges are surely magnified by the fact that it is the result of a recent merger of 22 legacy agencies, each of which brought with it its own policies, systems, processes, and culture.

The complexity of the Department's missions, coupled with the enormity of its management and operational challenges, requires

the close and continuing oversight that an 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, to guide resource allocation and prioritization, to set clear and achievable benchmarks for progress and success, and to enhance the Department's implementation of its critical mission.

H.R. 1817 is the first DHS authorization bill to be reported to the House since the creation of the Department in the Homeland Security Act of 2002 (P.L. 107–296), two and half years ago in the wake of the terrorist attacks of September 11, 2001. Given the pendency of the new Secretary of Homeland Security's comprehensive 90-day review of the Department's management, operations, and organization, the intent of this bill is not to make significant changes to the Department's overall budget and structure. Rather, the intent of this bill is to make some targeted and necessary improvements in the Department's operations, and to lay the foundation for a more comprehensive, annual review in collaboration with the Department.

In particular, H.R. 1817 will enhance terrorism-related information analysis, integration, and sharing, bolster efforts to develop and deploy critical anti-terrorism technologies, elevate the cybersecurity mission within the Department, fully fund 2,000 additional Border Patrol agents to help secure our Nation's vast borders against infiltration by terrorists or terrorist weapons, and enhance cargo and port security. Further, H.R. 1817 accomplishes these goals within a realistic budgetary framework, consistent with the House-passed Budget Resolution and the President's Fiscal Year 2006 budget request for the Department.

HEARINGS

Prior to the introduction of H.R. 1817, the Committee held numerous hearings on the Department of Homeland Security's Budget and the issues considered within H.R. 1817.

On Wednesday, April 13, 2005, the Full Committee held a hearing entitled "The Department of Homeland Security: Promoting Risk-Based Prioritization and Management." The Committee received testimony from The Honorable Michael Chertoff, Secretary, Department of Homeland Security.

On Thursday, February 10, 2005, the Subcommittee on Emergency Preparedness, Science, and Technology held a hearing entitled "The Proposed Fiscal Year 2006 Budget: Enhancing Terrorism Preparedness for First Responders." The Subcommittee received testimony from the Honorable Penrose "Parney" Albright, Ph.D., Assistant Secretary, Science and Technology Directorate, Department of Homeland Security; Mr. Matt A. Mayer, Acting Executive Director, Office of State and Local Government Coordination and Preparedness, Department of Homeland Security; and General

Dennis Reimer (Ret.), Director, National Memorial Institute for the Prevention of Terrorism.

On Wednesday, February 16, 2005, the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment held a hearing entitled "The Proposed Fiscal Year 2006 Budget: Building the Information Analysis Capability of DHS." The Subcommittee received testimony from Lt. General Pat Hughes (Ret.), Acting Under Secretary, Information Analysis and Infrastructure Protection, Department of Homeland Security.

On Wednesday, March 2, 2005, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity held a hearing entitled "Proposed FY 2006 Budget: Integrating Homeland Security Screening Operations." The Subcommittee received testimony from Mr. Jim Williams, Director, US-VISIT Program, Border and Transportation Security Directorate, Department of Homeland Security; Ms. Carol DiBattiste, Deputy Administrator, Transportation Security Administration, Department of Homeland Security; and Ms. Deborah J. Spero, Deputy Commissioner, Bureau of U.S. Customs and Border Protection, Department of Homeland Security.

On Wednesday, March 9, 2005, the Subcommittee on Management, Integration, and Oversight held a hearing entitled "CBP and ICE: Does the Current Organizational Structure Best Serve U.S. Homeland Security Interests?" Testimony was received from Dr. James Carafano, Senior Research Fellow, The Heritage Foundation; Mr. Michael Cutler, Former Senior Special Agent, U.S. Immigration and Naturalization Service; Mr. David Venturella, Former Director, Office of Detention and Removal Operations, U.S. Immigration and Customs Enforcement, Department of Homeland Security; Mr. T.J. Bonner, President, National Border Patrol Council; and public witnesses.

On Thursday, April 14, 2005, the Subcommittee on Management, Integration, and Oversight held a hearing entitled "The Need to Strengthen Information Security at the Department of Homeland Security." Testimony was received from Mr. Steven I. Cooper, Chief Information Officer, Department of Homeland Security; Mr. Gregory C. Wilshusen, Director, Information Security Issues Government Accountability Office; and public witnesses.

On Tuesday, April 19, 2005, the Subcommittee on Prevention of Nuclear and Biological Attack held a hearing entitled "DHS Coordination of Nuclear Detection Efforts, Part I." Testimony was received from public witnesses.

On Wednesday, April 20, 2005, the Subcommittee on Prevention of Nuclear and Biological Attack held a hearing entitled "DHS Coordination of Nuclear Detection Efforts, Part II." Testimony was received from Mr. Vayl Oxford, Acting Director, Domestic Nuclear Detection Office, Department of Homeland Security.

On Wednesday, April 20, 2005, Subcommittee on Management, Integration, and Oversight, held a hearing entitled "Management Challenges Facing the Department of Homeland Security." Testimony was received from Mr. Richard L. Skinner, Acting Inspector General, Office of the Inspector General, Department of Homeland Security; Mr. Norman Rabkin, Managing Director, Homeland Security and Justice, Government Accountability Office; the Honorable Asa Hutchison, Chairman of the Homeland Security Practice, Veneble, LLC; the Honorable James S. Gilmore, III, Chairman, Na-

tional Council on Readiness and Preparedness; and Mr. Clark Kent Ervin, Director, Homeland Security Initiative, The Aspen Institute.

On Wednesday, April 20, 2005, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity held a hearing on H.R. 285, the Department of Homeland Security Cybersecurity Enhancement Act of 2005. Testimony was received from public witnesses.

COMMITTEE CONSIDERATION

On Tuesday, April 19, 2005, the Subcommittee on Emergency Preparedness, Science, and Technology met in open markup session to consider a Committee Print entitled "To amend the Homeland Security Act of 2002 to provide for homeland security technology development and transfer." The Subcommittee ordered favorably reported to the Full Committee for consideration, without amendment, by voice vote. Provisions of this Committee Print were included within section 302 of H.R. 1817, as introduced.

On Wednesday, April 20, 2005, prior to introduction of H.R. 1817, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity met in open markup session to consider H.R. 265, the "Department of Homeland Security Cybersecurity Enhancement Act of 2005." The Subcommittee ordered the bill favorably reported to the Full Committee for consideration, without amendment, by voice vote. Provisions of H.R. 265 were included within subtitle B of Title III of H.R. 1817, as introduced.

On Tuesday, April 26, 2005, the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment met in open markup session to consider a Committee Print entitled "The Homeland Security Information Sharing and Enhancement Act of 2005." The Subcommittee ordered the Committee Print favorably reported to the Full Committee for consideration, without amendment, by voice vote. Provisions of the Committee Print were included within Title II of H.R. 1817, as introduced, and within the Manager's Amendment offered by Mr. Cox during the Full Committee consideration of H.R. 1817.

H.R. 1817 was introduced by Mr. Cox on April 26, 2005, and referred solely to the Committee on Homeland Security. Within the Committee on Homeland Security, H.R. 1817 was retained at the Full Committee.

On April 27, 2005, the Full Committee met in open markup session, a quorum being present, and ordered H.R.1817 favorably reported to the House of Representatives, amended, by a unanimous 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.

H.R. 1817, Department of Homeland Security Authorization Act for FY 2006; was ordered favorably reported to the House, amended, by unanimous Voice Vote.

The following amendments were offered:

A Managers Amendment offered by Mr. Cox (#1), was AGREED TO by Unanimous Consent.

An amendment offered by Mr. Thompson (#2), an Amendment in the Nature of a Substitute, was NOT AGREED TO by a recorded vote of 12 yeas and 16 nays (Record Vote No. 4)

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Thursday, April 21, 2005 Convened: 10:13 a.m.

Adjourned: 11:43 p.m.

Meeting on : Markup of H.R. 1817, Department of Homeland Security Authorization Act for Fiscal Year 2006

Amendment offered by Mr. Thompson (#2)

☐ Attendance ☒ Recorded Vote Vote Number: 4 Total: Yeas 12 Nays 16 Present

	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. Peter T. King New York		✓		*Ms. Jane Harman California*	✓		
Mr. John Linder Georgia		✓		*Mr. Peter A. DeFazio Oregon*	✓		
Mr. Mark E. Souder Indiana		✓		*Ms. Nita M. Lowey New York*			
Mr. Tom Davis Virginia		✓		*Ms. Eleanor Holmes Norton District of Columbia*	✓		
Mr. Daniel E. Lungren California		✓		*Ms. Zoe Lofgren California*	✓		
Mr. Jim Gibbons Nevada		✓		*Ms. Sheila Jackson-Lee Texas*			
Mr. Rob Simmons Connecticut		✓		*Mr. Bill Pascrell, Jr. New Jersey*	✓		
Mr. Mike Rogers Alabama		✓		*Mrs. Donna M. Christensen U.S. Virgin Islands*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mr. Bob Etheridge North Carolina*	✓		
Ms. Katherine Harris Florida				*Mr. James R. Langevin Rhode Island*	✓		
Mr. Bobby Jindal Louisiana				*Mr. Kendrick Meek Florida*	✓		
Mr. Dave Reichert Washington		✓					
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Mr. Cox California, Chairman		✓		Total	12	16	

An amendment offered by Mr. Weldon (#3), at the appropriate place in the bill, insert a new section entitled "Reestablishment of EMP Commission.", was WITHDRAWN by Unanimous Consent.

An amendment offered by Mr. Meek (#4), to add at the end a new title entitled "Accountability: Addressing Management Challenges of the Department of Homeland Security", was NOT AGREED TO by a recorded vote of 11 Yeas and 16 Yays (Record Vote No. 5).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Thursday, April 21, 2005 Convened: 10:13 a.m.

Adjourned: 11:43 p.m.

Meeting on : Markup of H.R. 1817, Department of Homeland Security Authorization Act for Fiscal Year 2006

Amendment offered by Mr. Meek (#4) add at the end a new title "Accountability Addressing Management Challenges of the Department of Homeland Security."

☐ Attendance ☒ Recorded Vote Vote Number: 5 Total: Yeas 11 Nays 16 Present

	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. Peter T. King New York		✓		*Ms. Jane Harman* *California*			
Mr. John Linder Georgia		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Mark E. Souder Indiana				*Ms. Nita M. Lowey* *New York*			
Mr. Tom Davis Virginia				*Ms. Eleanor Holmes Norton* *District of Columbia*	✓		
Mr. Daniel E. Lungren California		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Jim Gibbons Nevada		✓		*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Rob Simmons Connecticut		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Mike Rogers Alabama		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mr. Bob Etheridge* *North Carolina*	✓		
Ms. Katherine Harris Florida		✓		*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Bobby Jindal Louisiana				*Mr. Kendrick Meek* *Florida*	✓		
Mr. Dave Reichert Washington		✓					
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Mr. Cox California, Chairman		✓		Total	11	16	

An amendment offered by Mr. Young (#5), at the appropriate place in the bill, insert the following new section entitled "Transfer of Preparedness Functions to Under Secretary for Emergency Preparedness and Response", was WITHDRAWN by Unanimous Consent.

An amendment offered by Mr. Pascrell (#6), add at the end the following new title entitled "Enhancement of Emergency Preparedness", was NOT AGREED TO by a recorded vote of 10 Yeas and 18 Nays (Record Vote No. 6).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Thursday, April 21, 2005 Convened: 10:13 a.m.

Adjourned: 11:43 p.m.

Meeting on : Markup of H.R. 1817, Department of Homeland Security Authorization Act for Fiscal Year 2006

Amendment offered by Mr. Pascrell (#6) add at the end a new title "Enhancement of Emergency Preparedness."

☐ Attendance ☒ Recorded Vote Vote Number: 6 Total: Yeas 10 Nays 18 Present

	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. Peter T. King New York		✓		*Ms. Jane Harman* *California*			
Mr. John Linder Georgia		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Mark E. Souder Indiana		✓		*Ms. Nita M. Lowey* *New York*			
Mr. Tom Davis Virginia		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*			
Mr. Daniel E. Lungren California		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Jim Gibbons Nevada		✓		*Ms. Sheila Jackson-Lee* *Texas*	✓		
Mr. Rob Simmons Connecticut		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Mike Rogers Alabama		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mr. Bob Etheridge* *North Carolina*	✓		
Ms. Katherine Harris Florida		✓		*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Bobby Jindal Louisiana				*Mr. Kendrick Meek* *Florida*			
Mr. Dave Reichert Washington		✓					
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Mr. Cox California, Chairman		✓		Total	10	18	

An amendment offered by Mr. Etheridge (#7), add at the end a new section entitled "Report to Congress on Implementation of Recommendations Regarding Protection of Agriculture", was AGREED TO by Voice Vote.

An amendment offered by Mr. Souder (#8), at the appropriate place in the bill, insert the following new title entitled "Border and Transportation Security Reorganization", was WITHDRAWN by Unanimous Consent.

An amendment offered by Mr. Langevin (#9), add at the end a new title entitled "Title V-Preparing Against Biological Attack", was NOT AGREED TO by a recorded vote of 11 Yeas and 17 Nays (Record Vote No. 7).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Thursday, April 21, 2005 Convened: 10:13 a.m.
Adjourned: 11:43 p.m.

Meeting on : Markup of H.R. 1817, Department of Homeland Security Authorization Act for Fiscal Year 2006

Amendment offered by Mr. Langevin (#9) add at the end a new title "Preparing Against A Biological Attack."

☐ Attendance ☒ Recorded Vote Vote Number: 7 Total: Yeas 11 Nays 17 Present

	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. Peter T. King New York		✓		*Ms. Jane Harman* *California*			
Mr. John Linder Georgia		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Mark E. Souder Indiana		✓		*Ms. Nita M. Lowey* *New York*			
Mr. Tom Davis Virginia		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*			
Mr. Daniel E. Lungren California		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Jim Gibbons Nevada		✓		*Ms. Sheila Jackson-Lee* *Texas*	✓		
Mr. Rob Simmons Connecticut		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Mike Rogers Alabama		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mr. Bob Etheridge* *North Carolina*	✓		
Ms. Katherine Harris Florida		✓		*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Bobby Jindal Louisiana		✓		*Mr. Kendrick Meek* *Florida*	✓		
Mr. Dave Reichert Washington		✓					
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Mr. Cox California, Chairman		✓		Total	11	17	

An amendment offered by Mr. Smith (#10), at the end of title IV, add a new section entitled "Center of Excellence for Border Security", was AGREED TO by Voice Vote.

An amendment offered by Mr. Davis (#11), at the end of title IV of the bill, add the following new section entitled "Plan to Reduce Wait Times", was AGREED TO, as modified by a unanimous consent request by Mr. Davis, by Voice Vote. A Unanimous Consent request by Mr. Davis to consider the amendment en bloc with an amendment to, in section 202(e) add a new section (2) relating to statutory requirements, was not objected to.

An amendment offered by Mr. Dicks (#12), add at the end a new section entitled "Optimizing Technology to Enhance Homeland Security", was WITHDRAWN by Unanimous Consent.

An amendment offered by Mr. Simmons (#13), at the end of section 301, add the following new subsection (c) entitled "Topoff Prevention Exercise", was AGREED TO by Voice Vote.

An amendment offered by Ms. Sanchez (#14), at the end of the bill add a new section entitled "Customs-Trade Partnership Against Terrorism (C-TPAT) Program", was AGREED TO, as modified by a unanimous consent request, by Voice Vote. A Unanimous Consent request by Ms. Sanchez to strike all, except for sections 509(a)–509(e), was not objected to.

An amendment offered by Mr. Rogers (#15), at the appropriate place, insert the following new section entitled "Authorization of Appropriations for Training of State and Local Personnel in Border States Performing Immigration Functions", was AGREED TO by Voice Vote.

An amendment offered by Ms. Jackson-Lee (#16), at the end of the bill, add a new title entitled "Securing Our Land Borders", was NOT AGREED TO by a recorded vote of 11 Yeas and 16 Nays (Record Vote No. 8).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Thursday, April 21, 2005 Convened: 10:13 a.m.

Adjourned: 11:43 p.m.

Meeting on : Markup of H.R. 1817, Department of Homeland Security Authorization Act for Fiscal Year 2006

Amendment offered by Ms. Jackson-Lee (#16) add at the end a new title "Securing Our Land Borders."

☐ Attendance ☒ Recorded Vote Vote Number: 8 Total: Yeas 11 Nays 16 Present

	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. Peter T. King New York		✓		*Ms. Jane Harman* *California*			
Mr. John Linder Georgia		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Mark E. Souder Indiana				*Ms. Nita M. Lowey* *New York*			
Mr. Tom Davis Virginia		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*	✓		
Mr. Daniel E. Lungren California		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Jim Gibbons Nevada		✓		*Ms. Sheila Jackson-Lee* *Texas*	✓		
Mr. Rob Simmons Connecticut		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*			
Mr. Mike Rogers Alabama				*Mrs. Donna M. Christensen* *U.S. Virgin Islands*			
Mr. Stevan Pearce New Mexico		✓		*Mr. Bob Etheridge* *North Carolina*	✓		
Ms. Katherine Harris Florida		✓		*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Bobby Jindal Louisiana		✓		*Mr. Kendrick Meek* *Florida*	✓		
Mr. Dave Reichert Washington		✓					
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Mr. Cox California, Chairman		✓		Total	11	16	

An amendment offered by Mr. Reichert (#17), in section 301, add a new section (c) entitled "Consultation With First Responders", was AGREED TO by Voice Vote.

An amendment offered by Ms. Norton (#18), at the end of the bill, add a new title entitled "Security of Public Transportation Systems", was AGREED TO, as modified by a unanimous consent request by Mr. Cox, by Voice Vote. A Unanimous Consent request by Mr. Cox to strike all, except for sections 4 and 5, was not objected to.

An amendment offered by Mr. Pearce (#19), in section 102, insert a new section (b) relating to the priority of additional border agents, was WITHDRAWN by Unanimous Consent.

An amendment offered by Mr. Weldon (#20), in title III, insert a new section, a sense of Congress entitled "Interoperable Communications Assistance", was AGREED TO by Voice Vote.

An amendment offered by Mr. Markey (#21), add at the end a new title entitled "Securing Critical Infrastructure", was NOT AGREED TO by a record vote of 12 Yeas and 16 Nays (Record Vote No. 9).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Thursday, April 21, 2005 Convened: 10:13 a.m.

Adjourned: 11:43 p.m.

Meeting on : Markup of H.R. 1817, Department of Homeland Security Authorization Act for Fiscal Year 2006

Amendment offered by Mr. Markey (#21) add at the end a new title "Securing Critical Infrastructure."

☐ Attendance ☒ Recorded Vote Vote Number: 9 Total: Yeas 12 Nays 16 Present

	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. Peter T. King New York		✓		*Ms. Jane Harman* *California*	✓		
Mr. John Linder Georgia		✓		*Mr. Peter A. DeFazio* *Oregon*			
Mr. Mark E. Souder Indiana		✓		*Ms. Nita M. Lowey* *New York*	✓		
Mr. Tom Davis Virginia		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*	✓		
Mr. Daniel E. Lungren California				*Ms. Zoe Lofgren* *California*	✓		
Mr. Jim Gibbons Nevada		✓		*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Rob Simmons Connecticut		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*			
Mr. Mike Rogers Alabama		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mr. Bob Etheridge* *North Carolina*	✓		
Ms. Katherine Harris Florida		✓		*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Bobby Jindal Louisiana				*Mr. Kendrick Meek* *Florida*	✓		
Mr. Dave Reichert Washington		✓					
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Mr. Cox California, Chairman		✓		Total	12	16	

An amendment offered by Mr. Souder (#22), at the appropriate place in the bill, insert the following new title entitled "Shadow Wolves", was AGREED TO by Voice Vote.

An amendment offered by Ms. Harman (#23), insert at the end a new title entitled "Harnessing Intelligence", was AGREED TO, as modified by a unanimous consent request by Mr. Cox, and amended, by Voice Vote. A Unanimous Consent request by Mr. Cox to insert "tribal" after references to "State, and local government", was not objected to.

An amendment offered by Mr. Cox (#23A) to the amendment offered by Ms. Harman, to insert after page 3 a new section entitled "Protection of Information", was AGREED TO by Voice Vote.

An amendment offered by Mr. Young (#24), add at end a new title entitled "Denial of Transportation Security Cards", was AGREED TO by Voice Vote.

An amendment offered by Mr. DeFazio (#25), at the end of the bill add a new title entitled "Aviation Security", was NOT AGREED TO by a recorded vote of 13 Yeas and 19 Nays (Record Vote No. 10).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Thursday, April 21, 2005 Convened: 10:13 a.m.

Adjourned: 11:43 p.m.

Meeting on : Markup of H.R. 1817, Department of Homeland Security Authorization Act for Fiscal Year 2006

Amendment offered by Mr. DeFazio (#25) add at the end a new title "Aviation Security."

☐ Attendance ☒ Recorded Vote Vote Number: 10 Total: Yeas 13 Nays 18 Present

	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. Peter T. King New York		✓		*Ms. Jane Harman* *California*	✓		
Mr. John Linder Georgia		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Mark E. Souder Indiana		✓		*Ms. Nita M. Lowey* *New York*	✓		
Mr. Tom Davis Virginia		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*			
Mr. Daniel E. Lungren California		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Jim Gibbons Nevada		✓		*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Rob Simmons Connecticut		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Mike Rogers Alabama		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mr. Bob Etheridge* *North Carolina*	✓		
Ms. Katherine Harris Florida		✓		*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Bobby Jindal Louisiana		✓		*Mr. Kendrick Meek* *Florida*	✓		
Mr. Dave Reichert Washington		✓					
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Mr. Cox California, Chairman		✓		Total	13	18	

An amendment offered by Mr. Souder (#26), at the appropriate place in the bill, insert the following new section entitled "Report and Plan Regarding Information and Intelligence Sharing by Department of Homeland Security", was WITHDRAWN by Unanimous Consent.

An amendment offered by Ms. Jackson-Lee (#27), add at the end a new title entitled "Ensuring Diversity in Department of Homeland Security Programs", was WITHDRAWN, as amended by a unanimous consent request by Mr. Thompson, by Unanimous Consent. A Unanimous Consent request by Mr. Thompson to consider en bloc an additional amendment: add at the end a new title "Additional Provision", was not objected to.

An amendment offered by Mr. Pearce (#28), to insert a new section 404 relating to mobile communications coverage on the U.S.-Mexico border, was WITHDRAWN by Unanimous Consent.

An amendment offered by Mr. Markey (#29), add at the end of title IV of the bill a new section 403 entitled "Inspection of Cargo Carries Aboard Commercial Aircraft", was NOT AGREED TO by a recorded vote of 8 Yeas, 20 Nays, and 1 voting Present (Record Vote No. 11).

COMMITTEE ON HOMELAND SECURITY
U.S. House of Representatives
109th Congress

Date: Thursday, April 21, 2005 Convened: 10:13 a.m.

Adjourned: 11:43 p.m.

Meeting on : Markup of H.R. 1817, Department of Homeland Security Authorization Act for Fiscal Year 2006

Amendment offered by Mr. Markey (#29) add at the end of title IV of the bill a new section "403. Inspection of Cargo Carried Aboard Commercial Aircraft."

☐ Attendance ☒ Recorded Vote Vote Number: 11 Total: Yeas 8 Nays 20 Present 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. Peter T. King New York		✓		*Ms. Jane Harman California*	✓		
Mr. John Linder Georgia		✓		*Mr. Peter A. DeFazio Oregon*			
Mr. Mark E. Souder Indiana		✓		*Ms. Nita M. Lowey New York*	✓		
Mr. Tom Davis Virginia		✓		*Ms. Eleanor Holmes Norton District of Columbia*			
Mr. Daniel E. Lungren California		✓		*Ms. Zoe Lofgren California*		✓	
Mr. Jim Gibbons Nevada		✓		*Ms. Sheila Jackson-Lee Texas*			✓
Mr. Rob Simmons Connecticut		✓		*Mr. Bill Pascrell, Jr. New Jersey*		✓	
Mr. Mike Rogers Alabama		✓		*Mrs. Donna M. Christensen U.S. Virgin Islands*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mr. Bob Etheridge North Carolina*	✓		
Ms. Katherine Harris Florida		✓		*Mr. James R. Langevin Rhode Island*	✓		
Mr. Bobby Jindal Louisiana		✓		*Mr. Kendrick Meek Florida*			
Mr. Dave Reichert Washington		✓					
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Mr. Cox California, Chairman		✓		Total	8	20	1

An amendment offered by Mr. Weldon (#30), at the end of title I add a new section entitled "State and Local Terrorism Preparedness", was AGREED TO by Voice Vote.

An amendment offered by Mrs. Christensen (#31), insert a new Title entitled "Office of Tribal Security", was WITHDRAWN by Unanimous Consent.

An amendment offered by Mr. Weldon (#32), in section 302(b)(3), insert a new subsection 313(c) establishing a working group with the Secretary of Defense on military technologies, was AGREED TO by Voice Vote.

An amendment offered by Mrs. Christensen (#33), at the appropriate place, insert a new section entitled "Border Patrol Unit for Virgin Islands", was WITHDRAWN by Unanimous Consent.

An amendment offered by Mr. Meek (#34), add at the end a new section entitled "Authority of Chief Information Officer", was WITHDRAWN by Unanimous Consent.

An amendment offered by Mr. Thompson (#35), at the end of the bill add a new title entitled "Study of Applications Under Safety Act", was WITHDRAWN by Unanimous Consent.

An amendment offered by Mr. Markey (#36), In subtitle A of title II, add at the end a new section entitled "Sec. 203. Homeland Security Impact Review of Liquefied Natural Gas", was WITHDRAWN by Unanimous Consent.

An amendment offered by Ms. Jackson-Lee (#37), at the end of the bill insert a new section entitled "Report on Border Violence", was WITHDRAWN by Unanimous Consent.

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. 1817, the Department of Homeland Security Authorization Act for FY 2006 is to authorize appropriations for fiscal year 2006 for the Department of Homeland Security, and for other purposes.

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.1817, the Department of Homeland Security Authorization Act for FY 2006, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, a cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974 was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall

cause such estimate to be printed in the Congressional Record upon its receipt by the Committee.

FEDERAL MANDATES STATEMENT

An estimate of Federal mandates prepared by the Director of the Congressional Budget

Office pursuant to section 423 of the Unfunded Mandates Reform Act was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the Congressional Record upon its receipt by the Committee.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

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

Sec. 1. Short title

This Act may be cited as the "Department of Homeland Security Authorization Act for Fiscal Year 2006."

TITLE I—AUTHORIZATION OF APPROPRIATIONS

Sec. 101. Department of Homeland Security

This section authorizes the top-line funding level for the Department of Homeland Security (DHS) as a whole, consistent with the President's Fiscal Year 2006 budget proposal for DHS and the House-passed Budget Resolution. All other specific authorizations included in this Act are subsumed herein. Programs not specifically authorized in this Act are not affected.

Sec. 102. Border patrol agents

This section authorizes more than $1.9 billion for border control and security between ports of entry—which is $310 million above the President's proposed Fiscal Year 2006 budget for such purposes. These additional funds will permit the Secretary of Homeland Security, in Fiscal Year 2006, to fully hire, train, and equip the 2,000 additional Border Patrol agents originally authorized under the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108–458).

The Committee strongly believes that our Nation's top homeland security priority must be the prevention of terrorist attacks, and a critical component of such a strategy is ensuring the security and integrity of America's borders against those who would carry out such attacks and the means by which they would carry them out. Additional Border Patrol agents provide a significant deterrent to individuals seeking to illegally enter the United States, or to smuggle in terrorist weapons, and this increase in funding will bolster our Nation's apprehension capabilities by approximately 20 percent.

The Committee also strongly believes that this additional funding for Border Patrol agents must come from reducing funds for lower priority programs and activities within the Department of Homeland Security, given the realities of the Department's overall budget for Fiscal Year 2006. In subsequent sections of this Act, the Committee's other programmatic authorizations reflect offsets to cover the entire $310 million increase in this account.

Since the September 11, 2001, terrorist attacks, additional staff, resources, and coordination have closed gaps along parts of the border. However, operational control is still lacking over large sections of the Nation's border. As certain areas are fortified, illegal border activity is re-directed to other less-monitored areas. In deploying the additional 2,000 border patrol agents authorized in this section, the Secretary shall make every effort to ensure that the less-monitored sectors along the U.S. international border with Mexico and Canada are adequately staffed to combat increasing illegal border activity.

Further, and in light of the additional 2,000 new Border Patrol agents authorized under this section, the Committee directs the Secretary to conduct a risk assessment as to whether some of these new agents should be placed, on a permanent basis, in the Caribbean region, particularly in the United States Virgin Islands. There currently is no Border Patrol station in within the U.S. Virgin Islands. The station responsible for covering this area is the Ramey Sector, located in Puerto Rico. The United States Virgin Islands has 175 miles of coastal borders and is a gateway to the continental U.S. This region has been increasingly exploited by human and drug smugglers to move people and narcotics, undetected, into the U.S. mainland.

The Committee also has a great interest in the America's Shield Initiative (ASI). This program will significantly improve U.S. border control capabilities, and the Committee expects the Department to issue a robust Request for Proposal (RFP) that addresses the National and regional requirements for this program sometime this summer. The current activities on the border highlight the need for a holistic, flexible, and integrated solution that contains the right mix of people, process, technology, and infrastructure. The complexity and strategic importance of this program require that DHS give careful consideration to project management and oversight. The ASI mission of integrating disparate Federal, State, local and tribal jurisdictions and agencies to provide a national solution to border control is paramount. The Committee supports the significant increase in the President's proposed budget for this program, which reflects the urgency of this program.

Sec. 103. Departmental management and operations

Of the amount authorized under section 101, this section authorizes to be appropriated $634,687,000, in Fiscal Year (FY) 2006 for Department of Homeland Security (Department or DHS) management and operations.

Specifically, this section authorizes $44,895,000 for the DHS Regions Initiative. Section 706 of the Homeland Security Act of 2002 requires the DHS Secretary to develop and submit a plan to Congress for consolidating and co-locating the regional and field offices of DHS' legacy components. The plan was due to Congress in November 2003; however, the Department has not yet finalized and submitted this plan.

The Committee is advised that the regional structure is now under consideration during the Secretary's 90–day review of the Department's policies, programs, operations, and organization. It is expected that integration and consolidation of the regional offices will result in increased efficiencies, improved program delivery, and cost savings.

The Fiscal Year 2006 budget request includes a request for $50,000,000 to support the establishment of the DHS regional structure. The Committee recognizes, however, that it is unlikely that full development and implementation of the plan could occur in FY 2006. Therefore, the Committee reduces the requested budget increase by $5,000,000.

This section also authorizes $4,459,000 for the DHS Operational Integration Staff Initiative. The Committee recognizes that the Fiscal Year 2006 budget request includes an increase of $10 million to create a permanent Operational Integration Staff in the Office of the Secretary "to provide high-level coordination and integration." According to the budget request, the funding would be used to establish this staff as a "permanent entity." The Committee is advised that the Secretary already has established an Operational Integration Staff, referred to as "I-STAFF." The Committee is further advised that this staff includes at least 8 Full Time Employees (FTEs).

Integration of DHS is expected to result in increased efficiencies, reassignment of personnel to meet the Department's missions more effectively, and cost savings. These efficiencies and cost savings within the Department should allow the Secretary to shift resources to priority functions, rather than requiring an increase in FTEs for integration staff. Therefore, while the Committee strongly supports the integration function, the Committee reduces the proposed budget increase for this new, permanent entity by $5,000,000.

This section also authorizes $56,278,000 for the DHS Office of Security. The Committee strongly supports the role of the Office of Security in processing personnel security clearances and accesses, conducting security awareness education and training, and providing security accreditation of the Department's facilities and select information systems.

The Fiscal Year 2006 budget request includes a program increase of $39,445,000, which would more than double the budget for this Office to $61,278,000. The Committee recognizes, however, that provisions in the Intelligence Reform and Terrorism Prevention Act of 2004, enacted in December 2004, as P.L. 108–458, will help to

streamline clearance processing and reduce some of the burden on this Office. Therefore, the Committee believes a reduction of $5 million in the requested budget increase is warranted. The funding level authorized by the Committee would still more than double the budget of the Office, an increase the Committee believes is warranted due to the importance of the Office's mission and its increased workload.

The savings outlined above, $15 million in total, have been dedicated for increased Border Patrol agents, consistent with Section 102 of this Act.

Sec. 104. Critical infrastructure grants

The Committee authorizes to be appropriated $500,000,000 for Fiscal Year 2006 for grants and other assistance to improve critical infrastructure protection. This represents a $135 million increase over Fiscal Year 2005 for similar critical infrastructure grants, although it is $100 million lower than the President's request. The Committee is concerned that the Department still is not fully employing a risk-based strategy for distributing these critical infrastructure grants, and that the money that has been allocated in the past has often been used for security projects of marginal utility to terrorism preparedness. The Committee also remains concerned about the delay in use of critical infrastructure grant funds that previously have been awarded. This reduction of $100 million has been dedicated for increased Border Patrol agents, consistent with Section 102 of this Act.

The President proposes, in his Fiscal Year 2006 budget request, to combine all of the critical infrastructure grants into a single, risk-based program. While the Committee supports the concept of risk-based allocation, the Committee believes additional details about how a single critical infrastructure grant program would operate are necessary, and its authorization under this section is not meant to authorize, at this time, a single grant program.

Sec. 105. Research and development

Of the amounts authorized under section 101, this section authorizes appropriations for Fiscal Year 2006 for certain research and development (R&D) accounts.

Specifically, it authorizes appropriations of $76,573,000 to support chemical countermeasure development activities, a $24 million increase over Fiscal Year 2005 levels. The Committee supports continuing research in this area, but believes that not all of the proposed $49,000,000 increase in the President's budget is necessary. Accordingly, the Committee has reduced the proposed increase by $25,000,000. Of this amount, $20 million will be used to authorize additional Border Patrol agents, and $5 million of this reduction will be used to authorize additional funds for the SAFETY Act Implementation Office (discussed below).

With respect to the President's proposed Domestic Nuclear Detection Office (DNDO), this section authorizes appropriations of $197,314,000. The Committee strongly supports the intent of the President's initiative. However, given the Committee's concerns about the scope and authority of this new office, its over-emphasis on detection technology to prevent nuclear terrorism, and the likely inability of the new office to fully expend the total requested

amount during its first year, the Committee has authorized $30,000,000 less than the President's budget request of $227,000,000. The Committee notes that the authorized amount is still a $70,000,000 increase over Fiscal Year 2005 for comparable programs. This reduction of $30 million has been dedicated for increased Border Patrol agents, consistent with Section 102 of this Act.

This section also authorizes $10,000,000 for research and development of technologies capable of countering threats posed by man-portable air defense systems, including location-based technologies and non-commercial aircraft-based technologies. The Committee has authorized a sharp reduction in the funding for counter-MANPADS Research and Development (R&D) from the $110,000,000 proposed in the President's budget request ($49,000,000 above the Fiscal Year 2005 enacted level). Consistent with the budget views and estimates submitted by the Committee in March 2005 to the Committee on the Budget, the Committee believes that spending such a significant amount of funds on R&D and—most expensively—testing of aircraft-based counter-MANPADS systems is unjustified, absent a risk and cost assessment by either the Administration or the Congress supporting the actual deployment of such countermeasures. The Committee also believes that R&D funding in this area should be open to alternative technologies, which may provide more effective solutions to this threat at lower cost. Accordingly, the Committee has shifted $100 million from this account to pay for additional Border Patrol agents, which should help to decrease the ability of terrorists to smuggle anti-aircraft missiles into the United States.

Finally, this section authorizes $10,600,000 for the activities of the Science and Technology Directorate relating to the responsibilities described in subtitle B of title VIII of the Homeland Security Act of 2002 (P.L. 107–296) (6 U.S.C. 441 et seq.), commonly known as the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002. This is $5,000,000 more than the level proposed by the President, which would have reduced funding by $4,400,000 below Fiscal Year 2005 enacted levels.

Sec. 106. Border and transportation security

This section authorizes funding for the proposed Screening Coordination and Operations (SCO) Office at $826,913,000. The purpose of the SCO is to coordinate the enrollment and credentialing process for selected Department of Homeland Security (DHS) programs. The Committee supports the idea of the SCO and efforts to reduce costs by coordinating and consolidating similar processes in the transferred programs, which is consistent with reforms contained in Section 202 of this Act. Section 106, however, reduces the Fiscal Year 2006 budget request for this office by $20 million. The Committee strongly believes that this type of integration is not only necessary, but should help the Department achieve savings through efficiencies generated by the integration of multiple, overlapping programs. Therefore, the SCO should have sufficient resources to stand up and manage the new office without the need for additional expenditures and personnel, as called for in the President's budget request. The Committee is re-directing this $20 million to fund additional Border Patrol agents.

This section also authorizes funding for the weapons of mass destruction detection technology account at $100 million. This provides a $20 million increase above Fiscal Year 2005, although it is $25 million less than the Fiscal Year 2006 request. The Committee supports the deployment of such detection technology at U.S. ports of entry, but remains concerned about the escalating costs and delayed time frame for this program. The Committee also does not believe that the Department has a scientifically sound and risk-based deployment plan in place. For these reasons, the Committee has reduced the proposed increase for this program. From this reduction, $200 million will be re-directed to fund additional Border Patrol agents, and $5 million will be reserved to fund the Pre-Positioned Equipment (PPE) program. The PPE is one component of the Nation's plan to ensure that the necessary equipment is in place to respond to weapons of mass destruction attacks, but it was not funded in the President's budget request. The Committee urges the Department to propose specific funding for this program in Fiscal Year 2007, and to make sure that the program receives sufficient funding in Fiscal Year 2006 to maintain operations.

This section also authorizes $133,800,000 for the Container Security Initiative (CSI) for Fiscal Year 2006. The Committee generally supports this program, but is providing for certain reforms in other parts of this Act that require DHS to justify any further expansion of CSI based on a risk and cost-benefit assessment, particularly with respect to the need to deploy DHS personnel at such overseas ports. These requirements should generate cost savings in this program sufficient to continue appropriate expansion without additional resources in Fiscal Year 2006. To this end, this section provides for CSI funding levels only slightly higher than last year, and roughly $5 million below the President's Fiscal Year 2006 request. These savings will be re-directed to increase available funding for Border Patrol agents.

Sec. 107. State and local terrorism preparedness

Of the total amount authorized under section 101, this section authorizes appropriations for Fiscal Year 2006 for certain State and Local Terrorism Preparedness programs.

Specifically, it authorizes appropriations of $40,500,000 for the activities of the Office for Interoperability and Compatibility (OIC) within the Science and Technology (S&T) Directorate. This is $20,000,000 more than the level proposed by the President in his budget proposal. It is offset by an equal reduction to the President's request for discretionary grants for high-threat, high-density urban areas. Notwithstanding this reduction from the proposed level, the $1,000,000,000 authorized for such grants is a $115 million increase over Fiscal Year 2005.

The Committee recognizes that States and local governments, such as high-threat, high-density urban areas, require technical assistance and guidance to design, install, and operate comprehensive and effective interoperable communications systems. The OIC's guidance and technical assistance will help urban and other high-risk areas best utilize their grant funds for such purposes. Moreover, enhanced OIC capabilities will result in wiser spending decisions, effective communications improvements, and an efficient use of grant funds.

Sec. 108. Authorization of appropriations for training of State and local personnel in border States performing immigration functions

This section authorizes reimbursement to States along U.S. borders and coasts for the costs associated with having their state and local law enforcement personnel trained and certified by the Department of Homeland Security's (the Department or DHS) U.S. Immigration and Customs Enforcement (ICE) to enforce Federal immigration laws. Currently, immigration laws can be enforced only by Federal law enforcement officials, even when state and local authorities encounter persons, in the course of performing their routine law enforcement duties, that they suspect may not be in the U.S. legally. However, since 1996—when section 133 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 amended section 287 of the Immigration and Nationality Act (INA) and added subpart (g)—there has been authority allowing state and local law enforcement to be trained and certified by ICE, under voluntary agreements entered into between the Federal government and the participating State or local jurisdiction.

Specifically, section 287(g) of the INA authorizes the Secretary of Homeland Security to enter into agreements or Memoranda of Understanding (MOU) with any State or political subdivision for training to be qualified to perform functions of an immigration officer, including investigation, apprehension, and detention of undocumented aliens in the United States. So far, the Department has entered into three MOUs: the State of Florida in September 2002, the State of Alabama in September 2003; and the county of Los Angeles, California, in February 2005. Despite the success of these existing programs and interest by at least 14 other jurisdictions, expansion to other States and localities has stalled because of costs associated with training, including the costs associated with the time officers are away from their regular duties.

To address this issue and encourage further expansion of this program, this section authorizes $40 million to reimburse certain States and political subdivisions for the costs associated with their personnel attending such immigration training, including travel, transportation, and per diem meals and lodging during the training provided by ICE, and the costs of replacement personnel. The Committee has focused on States that are located along U.S. borders and coastline, where state and local law enforcement assistance can be of most value in helping to secure the Nation's borders against terrorists or other aliens seeking to unlawfully enter the U.S.

The Committee authorizes the funding from ICE's management and administration account, as that will provide maximum flexibility to the Department and not directly affect other ICE programs. These funds pay for expenses such as operation and maintenance of facilities and equipment, supplies and materials, rent, and other administrative support. The Committee believes that ICE should work to eliminate overlap and duplication in administrative functions at the headquarter level, and encourages the Secretary of Homeland Security to review such matters as part of his ongoing 90–day review of the Department's overall organization and management. Specifically, the Secretary should review the organizational structure of the Border and Transportation Security Direc-

torate (BTS), under which ICE resides, to determine how best to eliminate duplication of office management and overhead caused by having multiple offices for legislative affairs, public affairs, international affairs, and intelligence within BTS (including within ICE).

In Fiscal Year 2005, the enacted funding for ICE management and administration was $232,565,000, and the requested amount for Fiscal Year 2006 is $277,572,000—representing a net increase of $45 million dollars. In addition to the $45 million increase over last year's budget, ICE is also set to receive a substantial reprogramming of fiscal year funds from other elements of the Department, and may also receive additional funding in the Emergency Supplemental Appropriations bill soon to be considered by the Congress. Overall, the budget for ICE in Fiscal Year 2005 was $3.8 billion, and the President's request for Fiscal Year 2006 is $4.3 billion—representing a net increase of $519 million. Given these factors, the Committee believes that there is sufficient funding within ICE to reimburse States and local governments for assisting with the enforcement of Federal immigration law in border States, particularly with improved management and more streamlined operations.

TITLE II—TERRORISM PREVENTION, INFORMATION SHARING, AND RISK ASSESSMENT

Subtitle A—Terrorism Prevention

Sec. 201. Terrorism Prevention Plan and related budget submission

Subsection (a). Terrorism Prevention Plan

The Homeland Security Act of 2002 (P.L. 107–296) sets forth the missions of the Department of Homeland Security (Department or DHS), which include: (1) to prevent terrorist attacks within the United States; (2) to reduce the vulnerability of the United States to terrorism; and (3) to minimize the damage, and assist in the recovery, from terrorist attacks that occur within the United States. Despite the Department's primary mission to prevent terrorism, DHS has no department-wide plan solely focused on preventing a terrorist attack.

The Department currently is responsible for developing department-wide plans that address the latter two missions. Specifically, to reduce our vulnerability, DHS is developing the National Infrastructure Protection Plan (NIPP). The NIPP will serve as a blueprint for actions by the Department and its stakeholders to develop and implement a national effort to protect infrastructure across all sectors and reduce the vulnerability of the United States to terrorism. To coordinate efforts to assist in the recovery from a terrorist attack, DHS issued its National Response Plan (NRP) in December 2004. This plan establishes a single, comprehensive framework for the management of domestic incidents designed to minimize the damage and assist in the recovery of a terrorist attack.

Without a comprehensive plan dedicated exclusively to prevention, however, it is difficult for the Department and the Congress to assess the proper allocation of limited counterterrorism resources among prevention, vulnerability reduction, and response cannot be achieved. Therefore, this subsection requires the Sec-

retary to develop a Department of Homeland Security Terrorism Prevention Plan (TPP) that includes the Department's goals, objectives, milestones, and key initiatives to prevent acts of terrorism on the United States and its interests. The Secretary is required to submit the TPP to Congress no later than one year after the date of enactment of this Act, and on a regular basis thereafter as it is modified.

The TPP will include: the identification and prioritization of the most significant threats to, and terrorist groups threatening, the United States; an evaluation of the materials and methods that terrorists may use and the outcomes the terrorists aim to achieve; the process of coordination between DHS and the National Counter Terrorism Center; policies and procedures regarding how DHS will gather real-time information and incorporate it into counterterrorism activities; specific initiatives by DHS to identify threats, coordinate activities within the Department to prevent acts of terrorism, and share information with state and local governments and the private sector; the timeline for implementation of departmental information-sharing initiatives, such as the Homeland Security Information Network; and other terrorism prevention-related elements.

In formulating the TPP, the Secretary of DHS is required to consult with the heads of key Federal law enforcement and intelligence agencies, as well as State, county, and local law enforcement agencies the Secretary considers appropriate. The TPP will be prepared in both classified and unclassified forms.

Subsection (b). Annual Crosscutting Budget Analysis

In addition to formulation by the Department of Homeland Security (DHS) of a plan to prevent terrorist attacks on the United States, it is critical that limited homeland security resources are allocated towards the areas of greatest risk, and that sufficient emphasis is placed by DHS on activities and functions that are effective in preventing terrorist attacks on the United States and its interests.

To accomplish this goal, Congress and the public require a clear explanation of how DHS' budget is allocated among its various missions—both homeland security-related and non-homeland security-related missions. The Fiscal Year 2006 DHS budget request, however, lacks sufficient data in this regard, making it virtually impossible for Congress, the public, and even the Department's management to determine whether DHS is allocating its finite resources appropriately.

Therefore, this subsection requires the Secretary of Homeland Security to submit to Congress a crosscutting analysis of funding levels proposed for DHS programs by mission area, which will accompany the President's annual budget request. With respect to dual-purpose funding serving both homeland security and non-homeland security purposes, such as multi-duty personnel and shared capital investments, this subsection requires that such funding be analyzed and apportioned accordingly. The budget analysis will include separate displays for mandatory and discretionary appropriations.

In light of the importance of preventing terrorist attacks, this analysis will specifically identify DHS spending for: intelligence ac-

tivities generally; collection and use of intelligence and law enforcement operations that screen for and target terrorists; investigative, intelligence, and law enforcement operations that disrupt plans for terrorist acts and prevent the introduction of weapons of mass destruction into the United States; initiatives to detect potential or early stages of actual biological, chemical, radiological, or nuclear attacks; screening individuals against terrorist watch lists; screening cargo for potential compromise by terrorists or terrorist weapons; specific utilization by DHS of information sharing, both within the Federal Government and among Federal, State, and local governments to detect or prevent acts of terrorism; and initiatives to preempt, disrupt, and deter terrorist acts overseas intended to strike the United States. The prevention analysis also will include investments in technology, research and development, training, and communications systems that are designed to improve the performance of DHS in carrying out these functions.

Sec. 202. Consolidated background check process

The Department of Homeland Security has numerous security programs that pre-screen individuals by checking their names and biometric identifiers against terrorist watch lists and other criminal databases. Each of these programs has its own method of application, with a separate fee for each one. These programs often have their own enrollment centers, with some programs only having one or two sites per State. The Committee believes that the redundancies and inefficiencies in the application processes for these separate Department programs puts an unnecessary strain on the frequent travelers, workers, and businesses that conduct commerce across borders and within the U.S. They also provide an opportunity for terrorists to exploit any gaps between or among these various programs.

Section 202 of this Act directs the Secretary to address these redundancies and inefficiencies, by creating a single application process that will meet the security requirements for all of the voluntary and mandatory programs listed in the section and any additional programs that the Secretary may wish to include. The programs that are specifically included in this section are: the Transportation Worker Identification Credential (TWIC), the Hazmat Endorsement Credential vetting program, the Free and Secure Trade (FAST) Program, the NEXUS and SENTRI border crossing programs, and the Registered Traveler program of the Transportation Security Administration (TSA).

The list of included programs is intended to both specify the types of programs that should be included in the consolidated program, but also to give the Secretary flexibility in adding more programs as the Department progresses. The Committee encourages the Secretary to take into account this consolidated process in the future when creating or implementing any new screening, vetting, or credentialing program. The Committee specifically does not intend this list to include Federal security clearance applications, which are governed by a separate statutory and regulatory framework.

This section outlines four specific requirements for a single security screening process. The first is that the program must develop a single submission of security screening information that will

meet all the requirements of applicable Departmental programs, to the greatest extent practicable. By developing such an application, applicants who participate in more than one of these programs will not need to re-submit such information as biometrics and other personal data.

In carrying out this section, the Secretary should identify the commonalities of the application and screening processes for the included programs, and these commonalities should be leveraged to reduce the burden on applicants who apply to multiple programs, and to make it easier for applicants to apply to any of the programs. The Committee recognizes that some programs have requirements that do not apply across other programs. For example, the Registered Traveler program requires an in-person interview as part of the application process. The Committee does not intend for this language to be construed as altering that requirement.

The Committee has also found that the availability of centers or locations for submitting information for the programs can differ greatly program to program. In the case of the Hazmat Endorsement Credential, some drivers have reported the need to drive several hours to submit their information, losing valuable work time, during a process that can take two or three trips to complete. Thus, the second specific requirement under this section is that the Secretary permit applicants to apply to any of these programs at any designated center or through any designated process. Multiple program centers should have the ability to accept biometric information or personal application information and submit it to the Department. These centers should be made available to the users of any of the programs outlined in this section, to the extent that the center can accept the information required. The Committee does not see the need to establish separate centers across the country, collecting similar information, for multiple programs. This would also reduce the amount of funds needed for start-up or running of such programs.

The Committee also recognizes that there are other Federal clearances outside of the Department of Homeland Security that would meet the requirements of the included programs. Accordingly, the third specific requirement of this section directs the Secretary to ensure the process established above accepts any security clearance issued by another Federal agency, so long as the requirements for obtaining such a clearance are at least as stringent as those of the applicable DHS program or programs. For example, there are truck drivers who hold Federal security clearances to carry weapons munitions, who are then required to be vetted by TSA for a Hazmat credential. The Committee believes that this is not an efficient use of resources and is an unnecessary burden on such drivers.

Fourth, this section requires that the Secretary incorporate protection of privacy, confidentiality, record retention, and information security standards and procedures when creating the single application process.

This section also directs the Secretary to transmit to the Committee and the Senate Committee on Homeland Security and Governmental Affairs a description of the Department's plan for implementation no later than six (6) months after enactment, and re-

quires that the Secretary implement the process no later than twelve (12) months after enactment.

Finally, this section provides that all statutory requirements for the operation of the programs described in the program are not affected by this section, and that nothing in this section affects any statutory requirement relating to title III of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108–458) (50 U.S.C. 435b et seq.) (relating to Federal security clearance processing).

Subtitle B—Homeland Security Information Sharing and Analysis Enhancement

Sec. 211. Short title

This section names this subtitle as the "Homeland Security Information Sharing and Analysis Enhancement Act of 2005."

Sec. 212. Provision of terrorism-related information to private sector officials

Section 212 amends Sec. 201(d) of the Homeland Security Act of 2002 (P.L. 107–296) by requiring the creation and routine dissemination of analytic reports and products that provide specific information to private sector officials responsible for protecting their institutions from terrorist attacks or related consequences.

The Committee believes that the Department's Office of Information Analysis should use the Homeland Security Information Network (HSIN), authorized under section 220, as the normative means by which the Department disseminates the analytic reports and products required by this section to private sector officials.

Sec. 213. Analytic expertise on the threats from biological agents and nuclear weapons

This section amends Sec. 201(d) of the Homeland Security Act of 2002 (P.L. 107–296) by adding a provision making the Department of Homeland Security's Under Secretary for Information Analysis and Infrastructure Protection responsible for ensuring that the Office of Information Analysis acquires sufficient expertise to create, on an ongoing basis, analytic products (based on the analysis of homeland security information, as defined in section 892(f)(1)), specifically relating to the potential threat of terrorism involving the use of nuclear weapons and biological agents against the population and territory of the United States.

By including this section, the Committee intends to underscore the immediate importance of building, in the Department's Office of Information Analysis, a cadre of analysts with expertise focused on the risks associated with the potential use by terrorists of nuclear weapons and biological agents, the consequences of which would be unprecedented and unparalleled. In that connection, the Committee notes that analysis of homeland security information relating to terrorists' potential use of biological agents to attack the American people and territory should include systematic and sustained consideration of potential threats to, and associated measures to safeguard, the Nation's food and water supply from such attacks.

Sec. 214. Alternative analysis of homeland security information

Section 214 adds to subtitle A of title II of the Homeland Security Act of 2002 (P.L. 107–296) (6 U.S.C. 121 et seq.), a provision directing the Secretary to establish an alternative analysis process and assign an individual to ensure that the Department conducts alternative or "red-team" analysis of homeland security information that relates to potential acts of terrorism involving the use of nuclear weapons and biological agents.

The Committee notes, in this connection, that the Office of Information Analysis has already instituted an alternative analysis effort. The Committee is encouraged by this important initiative and wishes, by the mandate in this section, to ensure that the Department's "red team" analytic effort becomes permanent and non-elective. The Committee expresses no view on which of the Department's components the Secretary should assign principal responsibility for the alternative analysis responsibilities under this section. The Committee wishes to stress, nevertheless, the critical importance of ensuring that the Department's alternative analysis effort remains fully independent of the remainder of its analytic effort; otherwise, it has no potential to challenge, but will only mirror the analytic approaches and conclusions reflected in its more conventional analytic products. As this section makes clear, the Committee believes that the Department's alternative analysis efforts must focus particularly on the terrorist threats that entail the most catastrophic potential consequences—specifically, those involving attacks employing either nuclear weapons or biological agents.

Sec. 215. Assignment of information analysis and infrastructure protection functions

Section 215 requires the Department of Homeland Security's Under Secretary for Information Analysis and Infrastructure Protection (IAIP) to allocate the Under Secretary's existing responsibilities under section 201(d) of the Homeland Security Act of 2002 (P.L. 107–296) to the Assistant Secretary for Information Analysis (IA) and the Assistant Secretary for Infrastructure Protection (IP); both IA and IP will remain responsible for certain shared functions. IA is assigned 201(d)(1), (4), (7) through (14), (16), and (18). IP is assigned 201(d)(2), (5) & (6). Both IA and IP should have responsibilities for 201(d)(3), (15), (17), and (19). The Under Secretary for IAIP may assign additional duties relating to their assigned responsibilities to both IA and IP. Both Assistant Secretaries have coordinating responsibilities relating to their other assigned responsibilities under this section, with the Assistant Secretary for Information Analysis assigned special responsibility for exercising such coordinating functions with respect to elements of the intelligence community.

By more firmly delineating the statutory role of the Office of Information Analysis, the Committee is establishing a baseline by reference to which any future structural changes involving IAIP responsibilities could be made.

Sec. 216. Authority for disseminating homeland security information

The Homeland Security Act of 2002 (P.L. 107–296) gave the Secretary of Homeland Security special responsibility for providing in-

formation that relates to the prevention and deterrence of, preparation for, and response to potential acts of terrorism to State and local government personnel, tribal authorities, private sector officials, and the public. (See, e.g., Homeland Security Act of 2002, sec. 201(d)(9) and (11).) The Memorandum of Understanding Concerning Information Sharing signed on March 4, 2003 by the Attorney General (for all Federal law enforcement agencies), the Director of Central Intelligence (for members of the Intelligence Community), and the Secretary of Homeland Security (the MOU), notes, in section 4(b), that "the Federal government must, to the greatest extent possible, speak with one voice to state and local officials, private industry, and the public, in order to prevent confusion, mixed signals, and, potentially dangerous operational conflicts." The parties to the MOU agreed to require "the prior approval of the Secretary of Homeland Security" before any entities under their purview could disseminate terrorism- or other homeland security-related analysis to State, local, or private sector officials, or to the public, except in exigent circumstances or when such information is shared with federal, State and local law enforcement officials—provided that the Secretary of Homeland Security is given the earliest possible notice (MOU, at sec. 4(b)(ii) through (iv)). This one-voice priority is also reflected in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108–458), which at sec. 1011(a), specifically provides that the authority of the Director of National Intelligence does not extend to "the direct dissemination of information to State government and local government officials and private sector entities pursuant to sections 201 and 892 of the Homeland Security Act of 2002 (6 U.S.C. 121, 482)."

The Committee agrees that uncoordinated warnings send mixed messages to State, local, tribal, and private sector homeland security officials, as well as to the general public. Section 216 recognizes that when conveying homeland security information to State, local, tribal, and private sector officials, the Federal Government must, whenever possible, speak unambiguously and with a single voice. The Committee does not think State, local, and private sector officials should be left wondering which of multiple federal advisories to believe. Section 216, therefore, brings into the Homeland Security Act the agreement reflected in the MOU on Information Sharing noted above. This will help avoid the confusion that has resulted when federal agencies have failed to convey a single, coordinated evaluation of the homeland security threat situation clearly and through a single node to non-federal officials who exercise homeland security responsibilities.

Nothing in this or any other section of this subtitle is intended to suggest that the Department should not continue to prioritize, maintain, or, where appropriate, expand the sharing of information, including intelligence, relating to trade and customs revenue functions, to the extent that such sharing is among the customs revenue functions required to be maintained by section 412(b) of the Homeland Security Act of 2002.

Sec. 217. 9/11 Memorial Homeland Security Fellows Program

This section establishes a program named the 9/11 Memorial Homeland Security Fellows Program the purpose of bringing State, local, tribal, and private sector officials to become familiar with the

Homeland Security Operations Center (HSOC), including its mission and capabilities, and processes, as well as the personnel of the Offices of Information Analysis and Infrastructure Protection. This will enable the State, local, tribal, and private sector officials selected to interact more knowledgeably and efficiently with HSOC and other elements of the Directorate of Information Analysis and Infrastructure Protection (IAIP) on information sharing and other terrorism threat-related matters. The section:

- Establishes eligibility criteria for the program; those eligible must have homeland security-related responsibilities and possess a current national security clearance at the appropriate level.
- Limits the program to four 90–day iterations each year.
- Requires the Secretary to ensure that the number of fellows in residence at any time will not impede the activities of HSOC.
- Requires that a fellow's salary and benefits will continue to be paid by his or her home employer during the fellowship.
- Provides that each fellow will be reimbursed for round-trip, economy fare travel to and from their place of residence twice a month.

Subject to the selection criteria in this section, the Committee believes that the Secretary should seek to ensure that the individuals selected for participation in the 9/11 Memorial Homeland Security Fellows Program represent a diverse cross section of the State, local, tribal, and private sector officials who exercise homeland security-related responsibilities.

The Committee wishes to note, in addition, that individuals selected as Fellows under this section must not only possess a current national security clearance at the level required by the Secretary, but must also, before being given access to the Homeland Security Operations Center or to any classified information as a Fellow, execute the appropriate nondisclosure agreements and be provided and agree to observe appropriate security and handling instructions with respect to all information, reports, analytic products, and information concerning intelligence sources and methods, to which they may be given access during the period of their fellowship under this program.

The Committee believes that the Homeland Security Operations Center is a valuable information hub for the Department and, through the fellowship program established by this section seeks to ensure that HSOC and IAIP operations, products and personnel become more familiar to, and in tune with the needs of, State, local, tribal, and private sector homeland security officials.

Sec. 218. Access to nuclear terrorism-related information

This section ensures that the Assistant Secretary for Information Analysis receives promptly and without request all information obtained by the Department of Homeland Security that relates, directly or indirectly, to a threat of terrorism involving the potential use of nuclear weapons. It also ensures that such information is integrated and analyzed comprehensively, disseminated in a timely manner, including to cleared State, local, tribal, and private sector officials, and is used to determine what additional requests the Department should submit for further collection of information related to such threats.

The Committee notes that the responsibilities of the Department's Assistant Secretary for Information Analysis under this section do not impinge upon, limit, or affect in any way the role and responsibilities of the National Counter Proliferation Center established by section 1022 of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108–458). The Assistant Secretary is intended to exercise the Assistant Secretary's responsibilities under this section in a manner consistent with the role and responsibilities of the National Counter Proliferation Center under that Act.

Sec. 219. Access of Assistant Secretary for Information Analysis to terrorism information

The Committee believes that the Homeland Security Act of 2002 (P.L. 107–206) clearly envisioned that the Office of Information Analysis (IA) serve as the single office within the Department of Homeland Security where all terrorist threat-related information, regardless of its origin, is brought together for comprehensive analysis. To serve that role, IA must have access to all terrorist threat-related information collected by or otherwise in the possession of any of the Department's components.

Section 219 seeks to ensure that the Assistant Secretary for Information Analysis is routinely and without request given prompt access to all terrorism-related information collected by or in the possession of the Department, including direct access (where technologically feasible) to all databases of the Department that may contain such information.

Sec. 220. Administration of the Homeland Security Information Network

Through the Homeland Security Information Network (HSIN), the Department of Homeland Security seeks to provide a nationwide, real-time communications node for the Department, other Federal agencies, State and local officials, and private sector partners. HSIN currently uses the Joint Regional Information Exchange System (JRIES) framework. Section 220 authorizes the HSIN and assigns responsibility for developing and administering the network to the Secretary. It also assigns the Secretary the responsibility to ensure that the Network's information sharing systems utilize and are compatible with Federal, State, and local antiterrorism systems and protocols that have been or are being developed.

In making this new responsibility explicit, the Committee notes the excellent work done over the past several years by the Markle Foundation Task Force on National Security in the Information Age. The Markle Foundation Task Force was notable in that its members included top-flight private sector cyber-technologists, as well as experts on both national security and privacy issues drawn from every point on the national political spectrum. In its October 2002 report, the Markle Foundation Task Force wrote:

> As the new Department of Homeland Security takes shape, we have a unique opportunity to design and implement systems that will enable the best use of central and local resources. We have learned a great deal from the rapid growth in networks of all types in recent years. We can draw on our accumulated knowledge and our existing

networks to create a robust, decentralized, and networked national security framework. (Protecting America's Freedom in the Information Age (Oct. 2002), at p. 12).

The Task Force continued: "There currently is no coordinated strategy in the federal government for interaction with state and local entities. * * * The Department of Homeland Security must establish minimum guidelines and procedures for sharing and impose some order on a system that currently is almost entirely ad hoc" (id. At 75). Fourteen months later, the Markle Foundation Task Force issued its second report, which focused on how such a network should be created, noting that "the DHS has yet to articulate a vision of how it will link federal, state, and local agencies in a communications and sharing network" (Creating a Trusted Information Network for Homeland Security (Dec. 2003), vol. I at 8). The Committee understands the Homeland Security Information Network it is authorizing in this section as the vehicle by which the Department will link itself to Federal, State, local, tribal, and private sector entities in a mutually advantageous and durable homeland security information sharing network.

In recommending such a network, the Markle Foundation Task Force worked "from the premise that security and privacy can coexist" (Oct. 2002 report at 32). The Committee wishes to stress that the Department must, as it implements and expands the Homeland Security Information Network, pay close attention to maintaining privacy and civil rights, inasmuch as the Members of the Committee agree with the Task Force that "[t]he American way of life is a critical part of what our government is protecting when it provides for America's security" (Oct. 2002 report at 76).

The Committee understands that the technologies and applications necessary in order to establish and enhance the Homeland Security Information Network authorized by this section are, in large measure, already commercially available. The Committee wishes to encourage the Department to use such existing private sector technologies, whenever possible, in building and enhancing this Network. The Committee also believes that the Department of Homeland Security should make it a priority to link existing networks and applications wherever possible into the Homeland Security Information Network in order more rapidly and cost-effectively to expand the network. In addition, the Department must ensure that HSIN-users are provided the necessary training and support manage HSIN.

The Committee notes, finally, that the Homeland Security Information Network authorized by this section is understood and intended to be complementary to and wholly consistent with the terms of the Information Sharing Environment provided for in section 1016(b) of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108–458).

Sec. 221. IAIP personnel recruitment

The Directorate of Information Analysis and Infrastructure Protection (IAIP) of the Department of Homeland Security is required to conduct homeland security terrorist threat analyses and vulnerability assessments. To meet these responsibilities on an ongoing basis, it is essential that the Department develop an expert em-

ployed workforce of well-trained, seasoned analysts in the IAIP Directorate.

The Committee understands that the Department's Office of Information Analysis (IA) is struggling to compete with more established members of the intelligence community, as well as with private sector employers, to attract its needed analyst cadre from a relatively small pool of experienced and trained analysts. Because of the scope of its analytic responsibilities and because IA is a new player in the world of intelligence analysis and so does not yet have an established reputation to assist in its recruiting efforts, the Committee believes the Secretary must have the temporary authority to provide unique recruitment incentives.

This section requires the Secretary to approach this problem strategically and with an appropriate package of financial and other incentives. Incentives would be available for three years and include recruitment bonuses, as well as the authority to employ civil service annuitants with no diminution in the amount of the annuity (putting them in a category similar to military retirees). Without such a program, it is increasingly difficult to envision IAIP's employed analyst cadre attaining the critical mass and capabilities required to meet its Homeland Security Act mandates. The Committee envisions that these authorities may be used to fill positions requiring experts in fields such as linguistics, chemical, biological, radiological and nuclear sciences, regional and other specialized analysts as the Secretary determines necessary.

Section 221 amends Chapter 97 of title 5, United States Code, by adding after section 9701 a new section 9702 entitled Recruitment Bonuses. This section allows the Secretary, acting through the Under Secretary for IAIP, to pay a bonus to an individual in order to recruit an individual for a position that is primarily responsible for discharging the analytic responsibilities specified in section 201(d) of the Homeland Security Act of 2002, and is within the IAIP Directorate and would be difficult to fill without the bonus. The section contains other requirements, including:

the bonus may not exceed 50 percent of the annual rate of pay;

the bonus will be distributed as a lump sum;

recipient is subject to a written service agreement

appointees, non-career appointees in the Senior Executive Service, and those exempted from the competitive service are ineligible; and

authority terminates in 2008

This section also adds a new section 9703 entitled Reemployed Annuitants. Under this provision, an annuitant receiving an annuity from the Civil Service Retirement and Disability Fund may be employed in a position within the Directorate for Information Analysis and Infrastructure Protection without losing his or her annuity. This authority terminates in 3 years, but can be extended in one-year increments by the Secretary.

Sec. 222. Information collection requirements and priorities

This section amends section 102 of the Homeland Security Act of 2002 (P.L. 107–296) to add a provision that would make the Secretary of Homeland Security a member of any Federal Government interagency board that is responsible for establishing foreign collec-

tion information requirements and priorities. This section also establishes an interagency Homeland Security Information Requirements Board, chaired by the Secretary of Homeland Security, to oversee the process of establishing homeland security requirements and collection management for all terrorism-related and homeland security information collected within the United States.

Sec. 223. Homeland Security Advisory System

The color-coded designation of threat conditions the public has come to associate with the Homeland Security Advisory System (HSAS) originated in Homeland Security Presidential Directive-3 (March 11, 2002). The Homeland Security Act of 2002 assigned responsibility for administering the HSAS to the Under Secretary for Information Analysis and Infrastructure Protection of the Department of Homeland Security (P.L. 108–458, at sec. 201(d)(7)).

As currently administered, the Committee is concerned that the Homeland Security Advisory System fails to provide the public with critically necessary information. The Committee's oversight of the HSAS has confirmed the Committee's findings that the color-coded system is largely ignored by the general public and is confusing to law enforcement and emergency response personnel. Witnesses have testified that there is a general lack of specificity as to the type of attack and when and where the attack is likely to occur.

Section 223 amends Subtitle A of title II of the Homeland Security Act of 2002 by adding at the end a new section 205 entitled the Homeland Security Advisory System. This section:

- Directs the Under Secretary for IAIP to administer the Homeland Security Advisory System and provide advisories and alerts regarding threats to homeland security, including national, regional, local, and economic sector advisories and alerts, as appropriate.
- Requires that, in each advisory or alert regarding a threat, the appropriate protective measures and countermeasures are included.
- Requires whenever possible that each advisory or alert is limited to the specific region, locality, or economic sector at risk.
- Requires that the issuing of the any advisory or alert shall not use color designation as the exclusive means of specifying the homeland security threat condition.

While the Committee understands that the specificity, accuracy, classification, and quality of the available intelligence will necessarily dictate the specificity of the warning given, the Committee believes that the Department must be as specific it possibly can when issuing any threat advisory or alert under the HSAS.

The Committee strongly believes that the Homeland Security Advisory System must at all times be employed to convey to State, local, and tribal first responders and the general public the information required to inform them of what to look for and what to do to protect themselves and those within their area of responsibility during any period of heightened alert. Accordingly, this section requires that public advisories and alerts issued under the Homeland Security Advisory System include information on appropriate protective measures and countermeasures.

The Committee notes that this section does not purport to eliminate color-coding to indicate homeland security threat conditions—the Secretary should remain free to employ color-coding where the Secretary deems that appropriate—but it does require that the information provided under the Homeland Security Advisory System not be limited to indication of a color-coded threat condition. This section's primary intention is to ensure that advisories and alerts issued under the Homeland Security Advisory System provide information concerning the protective measures and countermeasures appropriate to the threat indicated in that advisory or alert.

Sec. 224. Use of open-source information

Open-source information—information from unclassified sources—covers a vast body of information of potential relevance to the fight against terrorism. Harnessing open source information is difficult because of its enormous breadth and volume. The Committee believes it can, nevertheless, serve as an important body of data for augmenting our understanding of the capabilities, plans, and intentions of terrorists, as well as of the vulnerabilities they may seek to exploit.

This section amends Section 201(d) of the Homeland Security Act of 2002 (P.L. 107–296) by adding a provision that requires the Assistant Secretary for Information Analysis to produce and disseminate reports and analytical products based on open-source information that does not require national security classification, and to ensure that such unclassified reports are, whenever possible, produced and disseminated contemporaneously with classified reports containing the same or similar information. The Committee believes that any open-source strategy developed within the Department should seek to take advantage of the numerous commercial technologies available, and should seek to expand existing partnerships with industry, academia, and other government agencies.

Sec. 225. Full and efficient use of open-source information

This section directs the Under Secretary for Information Analysis and Infrastructure Protection of the Department of Homeland Security to ensure that the Assistant Secretary for Information Analysis and the Assistant Secretary for Infrastructure Protection make full and efficient use of open-source information.

The Committee notes that, in requiring that the Assistant Secretary for Information Analysis and the Assistant Secretary for Infrastructure Protection make full and efficient use of open-source information, it intends to cover not only the acquisition and analysis of information from open—unclassified—sources, but also the dissemination of such open-source information and products to State, local, tribal, and private sector officials, as appropriate.

The Committee supports the Bio-surveillance Initiative that was established in 2005 as an unclassified collaborative initiative among the Department of Homeland Security (DHS), the Department of Health and Human Services (HHS), and the Department of Agriculture (USDA). The intent of the initiative is to gather, integrate, and analyze in real-time bio-surveillance data to improve the Federal government's capability to rapidly identify and characterize a potential bioterrorist attack.

The Information Analysis and Infrastructure Protection (IAIP) Directorate in the Department of Homeland Security has the specific responsibility to develop the capability for the real-time integration of bio-surveillance data from a variety of government sources. However, the Committee is concerned about the progress made in implementing this initiative, the potential difficulties of sharing information from such a wide variety of sources, and the roles and responsibilities of each participating agency.

Therefore, the Committee directs IAIP to provide a report, no later than 60 days after enactment of this Act, that describes the scope, cost, schedule, and key milestones for IAIP's portion of the Bio-surveillance Initiative. In addition, the report should: (1) Clarify the Department's role in this joint initiative; (2) describe the progress made in its implementation; (3) give a time frame for finalizing connectivity of the affected systems and giving IAIP the desired access to this biological surveillance information; (4) describe any changes that have been made to existing incident reporting or decision-making protocols; (5) provide a time frame for finalizing and fully implementing the information infrastructure to connect biological detection and collection systems; (6) outline the procedure that will be used to integrate intelligence with bio-surveillance data; and (7) outline the procedure that will be used to enable States and local agencies to report and receive relevant bio-surveillance data.

TITLE III—DOMESTIC PREPAREDNESS AND PROTECTION

Subtitle A—Preparedness and Protection

Sec. 301. National terrorism exercise program

Subsection (a) amends the Homeland Security Act (HSA) (P.L. 107–296) to assign the Office for Domestic Preparedness (ODP) with primary responsibility for designing, developing, performing, and evaluating terrorism preparedness exercises at the National, State, territorial, regional, local, and tribal levels of government. Specifically, ODP must ensure that such exercises test the Nation's capability to prevent, prepare for, respond to, and recover from acts of terrorism.

Subsection (b) establishes a new Subtitle J, entitled "National Terrorism Exercise Program," within Title VIII of the HSA, and directs the Secretary of Homeland Security, through ODP, to establish such a national program. The national program must: (1) Enhance coordination for terrorism preparedness across a broad cross-section of governmental entities, first responders, the private sector, and foreign entities; (2) be multidisciplinary and as realistic as practicable; (3) be based on current risk assessments, including credible threats, vulnerabilities, and consequences; (4) be as spontaneous as practicable; (5) be evaluated against performance measures and followed by corrective action; and (6) be assessed to learn and distribute best practices. Such a program also must assist State, territorial, local, and tribal governments in the design, implementation, and evaluation of their own exercises.

This subsection also directs the Secretary to perform periodic, national terrorism preparedness exercises involving top government officials from all levels of government (i.e. TOPOFF). Such exercises should test and evaluate the Nation's capability to prevent,

respond to, and recover from catastrophic acts of terrorism, especially those involving weapons of mass destruction. Moreover, the Secretary, in designing and conducting all exercises, must consult with a geographic (including urban and rural) and substantive cross-section of governmental and non-governmental first responder disciplines, including, as appropriate, Federal, State, and local first responder training institutions, representatives of emergency response providers, and State and local officials with an expertise in terrorism preparedness.

Subsection (c) directs the Secretary to conduct a specific TOPOFF exercise within one year of enactment that is focused solely on testing and evaluating the Nation's capability to detect, disrupt, and prevent catastrophic acts of terrorism. This additional exercise is not intended to replace the periodic, multi-purpose national terrorism exercises.

To test and evaluate the preparedness of as many first responders and top officials as possible in a cost-effective manner, the Committee encourages the Secretary to incorporate simulations as a component of the National Terrorism Exercise Program. Indeed, ODP should give priority to simulations that: (1) Use constructive modeling; (2) are geographically and architecturally specific for each scenario; (3) operate in "real time"; and (4) are not prescripted. The Committee also believes that the National Terrorism Exercise Program should reflect, as accurately as practicable, potential terrorist incidents, including biological terrorism. To that end, the Committee urges the Secretary to review the efficacy of existing laws, regulations, and guidelines governing the Department's ability to respond to potential biological events.

Sec. 302. Technology development and transfer.

Subsection (a) directs the Secretary of Homeland Security to complete the establishment of the Technology Clearinghouse within the Science and Technology (S&T) Directorate, as called for in the Homeland Security Act of 2002 (HAS) (P.L. 107–296), by no later than 90 days after the date of enactment. The Committee remains concerned about the delay in the Department of Homeland Security's (DHS) establishment of this clearinghouse, as mandated under the HSA.

Subsection (b) amends the HSA to require the Technology Clearinghouse to establish a homeland security technology and equipment transfer program to facilitate the identification, modification, and commercialization of technology and equipment for use by Federal, State, and local government agencies, first responders, and the private sector, to prevent, prepare for, and respond to acts of terrorism by:

conducting surveys and reviews of available technologies developed by the Department, other Federal agencies, the private sector, or foreign entities for potential use for homeland security purposes;

conducting or supporting research and development (R&D) activities of technologies identified to be transferred for homeland security purposes;

communicating the availability of such technologies, as well as their specifications, satisfaction of standards, and appro-

priate DHS grants for purchasing such technologies to governmental agencies, first responders, and the private sector;

coordinating all technology transfer activities of the S&T Directorate, including projects and grants awarded to the private sector and academia;

identifying technology transfer priorities for the S&T Directorate based on current risk assessments; and working in concert with first responders, foreign governments and international organizations, existing technology transfer programs, and State and local training institutions.

This subsection also directs the Secretary to establish a working group in coordination with the Secretary of Defense to advise and assist the Technology Clearinghouse in identifying military technologies that may be transferred for homeland security purposes. The working group may consist of representatives from the Department of Defense, Federal, State, and local first responders, and non-governmental organizations or private companies engaged in the R&D, testing, evaluation, or identification, of military technologies. The Secretary should select those private sector entities that have demonstrated prior experience and success in searching for, and identifying, technologies for other Federal agencies, and that possess expertise in homeland or national security technologies.

Subsection (c) requires the Department to report to Congress on its status in implementing the functions of the Technology Clearinghouse, as well as the S&T Directorate's progress in reviewing unsolicited technology proposals.

Subsection (d) precludes this section from being construed to expand the Department's R&D activities into human health-related R&D, which is prohibited under section 302(4) of the HSA.

The Committee supports the continued growth and operation of the Lessons Learned Information Sharing (www.LLIS.gov) system by the Office for State and Local Government Coordination and Preparedness, in conjunction with the National Memorial Institute for the Prevention of Terrorism, to promote the generation and dissemination of peer-validated lessons learned, best practices, and corrective actions across the entire range of emergency response and homeland security disciplines for all State, local, and tribal jurisdictions. The Committee believes that the LLIS.gov system may be one of several appropriate resources for the Technology Clearinghouse to make available or disseminate the results of technology surveys and technology transfer activities, including information and best practices on the use and availability of such technologies to emergency response providers.

The Committee notes that the Secretary, acting through the S&T Under Secretary, must consult with the Department's other Under Secretaries and the Director of the Office for Domestic Preparedness, with respect to this technology transfer program. The Committee encourages the S&T Under Secretary to include the U.S. Fire Administration, within the Emergency Preparedness and Response Directorate, during its consultations. The Committee further recommends that the Department, when coordinating and entering into agreements with other Federal agencies to facilitate effective commercialization of technologies, should consider utilizing

existing interagency entities, such as the Civil Applications Committee.

By emphasizing in this section the need for the Department to expedite the transfer of homeland security technologies to improve preparedness for acts of terrorism, the Committee is not suggesting that the Department should ignore the importance of technology development and deployment for its important non-homeland security missions. The Department should continue to prioritize, maintain, and expand, where appropriate, technology development and transfer activities related to such other missions, including trade and customs revenue functions consistent with the requirements under Section 412(b)(1) of the HSA.

Sec. 303. Review of antiterrorism acquisitions

Section 303 requires the Secretary of Homeland Security to study all Department procurements to identify those involving technology that has the purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, and to assess whether the technology is an appropriate candidate for the litigation and risk management protections of subtitle G of title VIII of the Homeland Security Act of 2002 (P.L. 107–296) (more commonly known as the "Support Anti-terrorism by Fostering Effective Technologies Act of 2002" (SAFETY Act)). In addition, the provision requires that, within 180 days of enactment, the Secretary must submit a report to Congress (1) describing the technologies identified as candidates for SAFETY Act protection, (2) prioritizing the technologies based on current risk assessment information, and (3) setting forth the specific actions the Department will take to encourage the sellers of those technologies to apply for SAFETY Act protections, and to ensure prioritized review of those applications by the Department.

The purpose of this provision is to encourage greater collaboration between elements of the Department involved in the procurement of antiterrorism technologies, on the one hand, and the personnel responsible for reviewing and approving SAFETY Act applications, on the other. In addition, this section is intended to ensure that the Department prioritizes and expedites SAFETY Act review of critical technologies that are the subject of pending and future Department procurements.

The Committee recommends that the Department's Chief Procurement Officer (CPO), in conjunction with the Office of SAFETY Act Implementation (OSAI), carry out this study and report. Successful completion of the directives contained in this section will require the Secretary to ensure that the CPO and OSAI have the full and timely cooperation of the Department's personnel within the procurement offices of all organizational elements of the Department, as well as personnel in the Office of Information Analysis with respect to the most current risk assessments.

The Committee believes this study will promote greater utilization of SAFETY Act protections as part of the Department's antiterrorism procurements, and result in prioritized and expedited SAFETY Act review for those antiterrorism technologies determined to be most critical based on current risk assessments and procurement needs. These steps also should improve general awareness of SAFETY Act benefits and encourage a higher number

of applications among private sector sellers of antiterrorism technologies.

The Committee also strongly believes that the Department must move more quickly to reduce the backlog in SAFETY Act applications. The SAFETY Act provides vital protection and incentives for the private sector to develop the technology needed to provide for effective homeland security.

Sec. 304. Center of Excellence for Border Security

This section directs the Secretary of Homeland Security (Department or DHS) to establish a university-based Center for Excellence for Border Security utilizing (Center) the same merit-review processes and procedures that the Science and Technology Directorate have established for selecting such centers. This Center shall prioritize its activities on the basis of risk to address the most significant threats, vulnerabilities and consequences posed by the Nation's borders and border control systems. Among other tasks, this Center should conduct research, examine border security technologies and systems, and provide education, technical, and analytical assistance for the Department to effectively secure the Nation's borders. The Committee also believes that this Center should examine the need to secure our borders from terrorists in a cost-effective manner, and how to achieve security without impeding legitimate trade and travel or adversely impacting the economic and social stability of surrounding communities.

The Committee notes that the Homeland Security Centers of Excellence program, administered by the DHS Science & Technology Directorate, is establishing university-based centers for multi-disciplinary research to address critical homeland security missions. Centers of Excellence bring together leading researchers, scientists, and technical experts to focus on the most significant terrorist threats facing our country. To ensure the Centers include the broadest range of expertise available nationally, the Under Secretary for Science & Technology shall, to the maximum extent practicable, review on an ongoing basis the applicant pool for the Centers of Excellence program to ensure that a diverse cross-section of our nation's higher educational institutions is represented. If the Under Secretary finds that institutions that traditionally serve minority or under-represented populations are not adequately reflected in the applicant pool, the Under Secretary shall actively undertake efforts to inform these institutions about the opportunities to participate in the Centers of Excellence program.

Sec. 305. Requirements Relating to the Container Security Initiative (CSI)

This section requires the Secretary of Homeland Security to conduct risk assessments on all foreign ports where the Container Security Initiative (CSI) program currently is operating, and any future port to which the Department of Homeland Security (Department or DHS) may consider expanding the program. CSI is a Departmental program that "pushes our borders out" by partnering with selected foreign ports to target and inspect containers traveling to the U.S. prior to loading at the foreign port.

The purpose of this section is to ensure that DHS personnel and resources are utilized in the most cost-effective manner to combat

the threat from the potential compromise of cargo containers by terrorists or terrorist weapons. The Committee is concerned that the CSI program lacks an overall strategy for designating CSI ports, and for deploying U.S. Customs and Border Protection (CBP) personnel to foreign ports—which is an expensive proposition and must be sufficiently cost-justified in terms of benefits to the U.S.

This section also authorizes DHS to use appropriated program funds to purchase, install, and provide training for screening equipment at foreign ports, under standards established by the Secretary. Such funding should help to improve the reliability of foreign inspections conducted under this program.

Finally, this section requires that containers arriving in the U.S. from a CSI port undergo the same level of inspection for potential compromise by terrorists or terrorist weapons as containers arriving from non-CSI ports, unless CBP personnel under the CSI program have verified that the targeted containers were inspected overseas for such purposes and found not to have been compromised by terrorists or terrorist weapons.

Sec. 306. Security of Maritime Cargo Containers

This section requires the Secretary of Homeland Security to issue container security regulations in accordance with the recommendations of the Maritime Transportation Security Act Subcommittee of the Advisory Committee on Commercial Operations (COAC), within six months after the date of enactment. Many security experts believe that the container supply chain is vulnerable to being exploited by terrorists. One of the major vulnerabilities is the integrity of containers as they are shipped from a foreign manufacturer to the United States. The COAC recommendations were developed with input from major stakeholders in the intermodal transportation and retail industries, and will help to ensure that containers are not susceptible to terrorist exploitation. Given that the container supply chain is global in scope, this section requires the Secretary to work with international organizations and foreign governments to ensure that the standards established by the Department are consistent with those being developed internationally.

This section also requires the Secretary to consolidate the Department's various container security technology and demonstration programs. The Department has several container security programs that appear to be redundant, such as Operation Safe Commerce, the Smart Box Initiative, and other container security programs in the Science and Technology Directorate. The Committee believes that consolidating these programs will result in savings and synergies, and will improve the Department's efforts to coordinate with industry in the development of technologies that will strengthen container security in the long term.

This section also authorizes the Secretary to carry out a demonstration project that integrates various non-intrusive inspection technologies. Currently, the Department uses two separate inspection technologies to screen containers. The Department deploys radiation portal monitors, which scan a container for radioactive or nuclear material. The Department also uses gamma-ray inspection technologies, which show the contents of a container similar to an X-ray. This section would permit the Department to evaluate whether these technologies can be integrated in a way that will

maximize a U.S. Customs and Border Protection (CBP) inspector's ability to detect a weapon of mass destruction or its components in a container.

Sec. 307. Security Plan for General Aviation at Ronald Reagan Washington National Airport

Not later than 180 days after the date of enactment, the Secretary of Homeland Security is directed to implement Section 823(a) of the Vision 100—Century of Aviation Reauthorization Act (P.L. 108–176). This requires the Secretary to develop and implement a security plan to permit general aviation aircraft to land and take off at Ronald Reagan Washington National Airport. In developing this plan, the Secretary shall consider reasonable requirements to ensure the security of both the operations at the airport and the security of the National Capital Region.

The Committee urges the Secretary to develop a plan to address any impact upon the U.S. Customs and Border Protection's Air and Marine Operations currently operating out of Reagan National Airport, including the considerations and feasibility of relocating such operations within the Flight Restricted Zone.

The Committee is concerned about the ongoing operational and economic impact associated with the 90–mile area of the Washington, D.C. Air Defense Identification Zone (ADIZ), and encourages Department of Homeland Security officials to work with other relevant agencies to update the reports and operational improvements called for in Section 602 of P.L. 108–176.

Sec. 308. Interoperable Communications Assistance

This section states that it is the Sense of the Congress that the Department of Homeland Security should implement, as expeditiously as possible, the initiatives assigned to the Office for Interoperability and Compatibility (OIC) under section 7303 of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108–458). Specifically, OIC should: (1) establish a comprehensive national approach to achieving public safety interoperable communications; (2) issue letters of intent to commit future funds for jurisdictions through existing homeland security grant programs, as appropriate, to encourage long-term investments in improving interoperability; (3) provide technical assistance to urban and other high-risk areas; and (4) complete a report to Congress on the Department's plans for accelerating the development of national voluntary consensus standards for public safety interoperable communications by no later than 30 days after enactment of this Act.

Sec. 309. Report to Congress on implementation of recommendations regarding protection of agriculture

On January 30, 2004, President Bush issued Homeland Security Presidential Directive-9 (HSPD–9) focusing on the defense of U.S. agriculture and food infrastructures against acts of terrorism. The directive establishes a national policy to defend the agriculture and food system against terrorist attacks, including specific measures for the development of a methodology for identifying and prioritizing critical agriculture assets, systems, and functions, and for sharing protection responsibility with State and local governments and the private sector. This is a shared mission between

several Federal partners, with specific functions and responsibilities assigned to the Secretary of Homeland Security (DHS).

The Government Accountability Office (GAO) recently issued a report evaluating the progress of DHS and other Federal agencies in implementing the responsibilities assigned under HSPD–9 and related executive directives. The GAO report observed progress made by DHS, but also identified several areas for improvement.

This section requires the Secretary of Homeland Security to submit a formal progress report within 120 days of passage of this Act, describing the actions that the Department plans to take to implement the recommendations made by the GAO report that are relevant to the Department's current statutory mandates and executive directives.

Subtitle B—Department of Homeland Security Cybersecurity Enhancement

Sec. 311. Short title

Section 311 entitled this subtitle as the "Department of Homeland Security Cybersecurity Enhancement Act of 2005".

Sec. 312. Assistant Secretary for Cybersecurity

The Committee believes that it is essential for the Department of Homeland Security (Department or DHS) to establish a cybersecurity framework to support the Nation's economy and security. Sophisticated cyber threats continue to emerge, and cyber attacks have increased dramatically in recent years. It has become clear that the United States needs to develop and maintain a comprehensive cybersecurity strategy.

Cybersecurity is a critical thread that cuts across every single infrastructure sector; it is the underlying foundation for the operation of business and government functions. Unlike physical vulnerabilities, cybersecurity vulnerabilities and threats can change in seconds and protective measures can become obsolete just as quickly. As the February 2003 President's National Strategy to Secure Cyberspace (the National Strategy) states:

> A network of networks directly supports the operation of all sectors of our economy—energy (electric power, oil, gas), transportation (rail, air, merchant marine), finance and banking, information and telecommunications, public health, emergency services, water, chemical, defense industrial base, food, agriculture, and postal and shipping * * * They also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, and radars. (National Strategy, p. 21.)

To ensure that the Department addresses these concerns systematically and with the requisite sense of urgency, Section 312 of this Act elevates the National Cybersecurity mission within DHS' Directorate for Information Analysis and Infrastructure Protection (IAIP)—creating an Assistant Secretary for Cybersecurity, who will have primary authority for all DHS IAIP cybersecurity-related critical infrastructure programs, including policy formulation and program management.

The Assistant Secretary's responsibilities will, among other things, include the establishment and management of a national

cybersecurity response system, a national cybersecurity threat and vulnerability reduction program, and a national cybersecurity awareness and training program. These responsibilities are based primarily on the President's National Strategy to Secure Cyberspace. The Assistant Secretary will help to coordinate cybersecurity activities across critical infrastructure elements, other DHS organizations, and with state and local governments. The Assistant Secretary will be in a position to provide critical input into national level policy decisions in this area. And elevating the position to the Assistant Secretary level will enable DHS to provide a single, visible point of contact within the Federal government, instead of multiple overlapping points of contact, to improve the interface with the private sector—which owns and operates roughly 85 percent of the Nation's critical infrastructure.

The Committee recognizes that the Assistant Secretary will have to work closely with the Assistant Secretary for Infrastructure Protection, given the interrelationship between the physical and cyber aspects of critical infrastructure protection. Nonetheless, the Committee disagrees with the contention that cybersecurity must remain within the Office for Infrastructure Protection in order to ensure such coordination. The Committee believes that there are other ways to ensure such coordination without making cybersecurity simply a subset of infrastructure protection generally.

In providing the general authority of the Assistant Secretary for Cybersecurity, it is the Committee's intent that all cybersecurity-related critical infrastructure protection programs operated by the United States Secret Service and Immigration and Customs Enforcement (ICE) Cyber Crimes Center will remain under the primary management and control of those respective organizations. Both organizations continue to provide leadership in building partnerships with private industry, academia and law enforcement agencies at all levels. In addition, nothing in this section is intended to alter or affect the responsibilities of the Department's Chief Information Officer with respect to the security of DHS' own critical information systems.

In addition, nothing in this section is meant to affect the operational authority and control by U.S. Customs and Border Protection over the Automated Commercial Environment (ACE) program or other Internet and technology programs under CBP's supervision prior to enactment of this Act.

The Committee encourages the Assistant Secretary for Cybersecurity 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 the States to conduct risk and needs assessments that take into account the multitude of threats to relevant cyber systems. The Assistant Secretary should encourage coordination with State Homeland Security Directors, State Chief Information Officers, and the Office for Domestic Preparedness within DHS to develop and promulgate a consistent methodology for developing such strategies.

This section also provides the Assistant Secretary with primary authority over the National Communications System. Organization-

ally, DHS treats telecommunications separately from information technology, thus dividing the mission and operations. Given the rapid convergence of data and telephony, however, DHS needs to have one comprehensive and coherent mission element. That said, this section allows for the highly effective telecommunications mission to remain intact within the National Communications System. This organization will allow a gradual transitioning as cyber and telecommunications continue to merge, while also ensuring strategic policy and program direction established under one Assistant Secretary.

The Committee also recognizes the importance of computer network security in protecting sensitive information. One element of securing network information is ensuring the identity of users. Technologies currently exist to strengthen user authentication (e.g., "passkeys" that require a biometric identifier or provide an ever-changing code that must be entered along with user name and password). To ensure appropriate access, these types of tools must be employed before users can access a system or information. The Committee is aware that, in addition to authenticating network users, it is now possible to authenticate devices that access computer networks, significantly enhancing security. The Committee, therefore, encourages the Department to examine device authentication alternatives for security and cost-effectiveness, and to incorporate device authentication in its computer networks and recommended best practices for other agencies and the private sector.

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 work with the private sector and academia to determine the best mechanisms for developing a distribution system for cybersecurity best practices and benchmarks.

Sec. 313. Cybersecurity defined

This section provides an authoritative definition for the term "cybersecurity" for use within the Department and the Homeland Security Act of 2002 (P.L. 107–296). The term "cybersecurity" is defined as the prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communication services, wire communications, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. This definition references terms from Federal statutes used by the U.S. Justice Department to prosecute electronic crimes:

- the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;
- the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

• the term "electronic communications system" means any wire, radio, electromagnetic, photo-optical or photo-electronic facility for the transmission of wire or electronic communications, and any computer facility or related electronic equipment for the electronic storage of such communications;
• "electronic communication service" means any service that provides to users thereof the ability to send or receive wire or electronic communications;
• "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce; and
• "electronic communications" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce. (See 18 U.S.C. 1030 and 18 U.S.C. 2510.)

From a security standpoint, this definition recognizes the convergence of emerging technologies, particularly between information technology and telecommunications. Technology is increasingly allowing individuals to transmit voice communications via the Internet and electronic data through wire lines. The Committee believes that there must be a comprehensive and consistent approach to securing these two types of networks, as well as future types of networks that might emerge. Given the rapid convergence of technology, the Committee strongly urges the Department to use this definition to guide its mission and policy functions.

Sec. 314. Cybersecurity training programs and equipment

Subsection (a) permits the Secretary of Homeland Security, acting through the Assistant Secretary for Cybersecurity, to establish a program, in conjunction with the National Science Foundation (NSF), to award grants to institutions of higher education (and consortia thereof) to: (1) establish or expand professional development programs in cybersecurity; (2) establish or expand associate degree programs in cybersecurity; and (3) purchase equipment to provide training for the professional development and associate degree programs.

Subsection (b) directs the Secretary, acting through the Assistant Secretary and in consultation with the NSF, to establish goals for the grant program and criteria for awarding grants. The Director of the NSF shall operate the program consistent with the established goals and criteria.

Subsection (c) specifies that the grants should be awarded on a competitive, merit-reviewed basis. In awarding the grants, the Director also shall, to the extent practicable, ensure geographic diversity and the participation of women and underrepresented minorities.

Subsection (d) provides that, of the amount authorized for the Department of Homeland Security in section 101, subsection (d) authorizes $3,700,000 for carrying out this section.

Subsection (e) contains relevant definitions.

The Committee recognizes that the threat to, and vulnerabilities of, our Nation's computer systems have increased the need for an educated and skilled workforce in the area of information security. System administrators and computer professionals are the first line of defense against cyber attacks. In order to create an educated workforce, however, the United States must have in place educational programs to provide future information technology professionals with specialized skills in information security. This new grant program will help us achieve that goal by providing hands-on training for a new generation of cybersecurity specialists.

Sec. 315. Information security requirements and OMB responsibilities not affected

This section clarifies that this subtitle, creating an Assistant Secretary for Cybersecurity within the Department of Homeland Security (DHS), does not affect any Office of Management and Budget (OMB) responsibilities under any Federal law, including Chapter 35 of title 44, United States Code, known as the Paperwork Reduction Act; the Clinger-Cohen Act of 1996 (divisions D and E of P.L.—104–106), including the provisions of law enacted by amendments made by that Act; and the Federal Information Security Management Act of 2002 (title III of P.L. 107–347), including the provisions of law enacted by amendments made by that Act. The role of the Assistant Secretary within DHS is not meant to duplicate OMB's existing role with respect to the security of Federal information systems, but rather to provide an operational program element that works with owners and operators of critical cyber infrastructures to enhance information security.

Subtitle C—Security of public transportation systems

Sec. 321. Security best practices

This section requires the Secretary of Homeland Security to partner with public transportation stakeholders and public officials to develop and disseminate security-related best practices for public transportation systems. The attack that occurred on a commuter train in Madrid, Spain on March 11, 2004, exposed the vulnerabilities of the U.S. public transportation system. The various systems of rail and mass transportation are vulnerable because of their inherent openness, size, and the need to operate in a timely manner to facilitate the travel of millions of passengers on a daily basis. This section will allow the Secretary of Homeland Security to receive input on the most effective security measures to be taken by transportation authorities, in order to develop these measures into a set of practices that can be applied nationwide.

The Committee also is concerned about the security of extremely hazardous materials in transportation. The security of these materials presents a challenge for the Department of Homeland Security as it must balance security with the free flow of commerce.

The Committee encourages the Secretary to improve the Department's efforts, in consultation with the Secretary of Transportation, to enhance the security of extremely hazardous materials shipments, as part of the broader effort to secure the Nation's transportation systems. The Committee believes the Secretary should con-

tinue to work with industry to research and implement ways to improve the physical security of rail cars and tanks carried by trucks containing extremely hazardous materials, to revise and implement existing extremely hazardous materials security plans to include the most current information and practices, to assist coordination between first responders and shippers of extremely hazardous materials, and to help develop and implement security training programs for employees. The Secretary should work with the Department of Transportation, State and local governments, and industry, to ensure that local jurisdictions have adequate response plans in place.

Sec. 322. Public awareness

This section requires the Secretary to partner with stakeholders to develop a national plan for public awareness of transportation security risks, which will increase the awareness and vigilance of public transportation employees and the riding public.

Subtitle D—Critical infrastructure prioritization

Sec. 331. Critical infrastructure

This section requires the Secretary of Homeland Security to complete the prioritization of critical infrastructure no later than 90 days after enactment. To be listed as priority critical infrastructure under this section, the Secretary must find that all of the following criteria for prioritization apply: the likelihood of the threat of terrorist attack, based on information received by the Department of Homeland Security's (DHS) Office of Information Analysis regarding the intentions and capabilities of terrorist groups and other potential threats; the likelihood that, due to vulnerabilities, such an attack would cause the destruction or significant disruption of such infrastructure; and the likelihood that such an attack would result in a substantial number of human deaths or serious bodily injuries, a significant adverse impact on the national economy, or a significant adverse impact on the national security. The Committee finds that it is necessary that the complete prioritized list of critical infrastructure be based on the above criteria to ensure that only high-risk critical infrastructure is included.

The Committee is concerned about the speed at which the Department is presently compiling and prioritizing its critical infrastructure list, and expects this section will ensure the process is completed adequately and in a timely fashion. In carrying out this section, the Secretary shall coordinate with other agencies and the private sector as necessary.

In conducting the prioritization of critical infrastructure required by subsection (a) of this Section, the Secretary shall review the appropriate sector-specific sections of the list with the appropriate information sharing and analysis organization, as defined by section 212(5) of the Homeland Security Act of 2002. The Secretary shall receive the organizations' recommendations for changes no later than 21 days before finalizing the list of critical infrastructure priorities.

The Committee also is concerned about the security of extremely hazardous materials in transportation. The security of these mate-

rials presents a challenge for the Department of Homeland Security as it must balance security with the free flow of commerce.

The Committee encourages the Secretary to improve the Department's efforts, in consultation with the Secretary of Transportation, to enhance the security of extremely hazardous materials shipments, as part of the broader effort to secure the Nation's transportation systems. The Committee believes the Secretary should continue to work with industry to research and implement ways to improve the physical security of rail cars and tanks carried by trucks containing extremely hazardous materials, to revise and implement existing extremely hazardous materials security plans to include the most current information and practices, to assist coordination between first responders and shippers of extremely hazardous materials, and to help develop and implement security training programs for employees. The Secretary should work with the Department of Transportation, State and local governments, and industry, to ensure that local jurisdictions have adequate response plans in place.

Sec. 332. Security review

This section requires the Secretary of the Department of Homeland Security to review existing security plans for securing the specific facilities included in the prioritized list, to recommend changes to existing security plans, and to coordinate and contribute to critical infrastructure protective efforts of Federal, State, and local agencies and the private sector as set out in Homeland Security Presidential Directive 7 (HSPD–7, Dec. 17, 2003). Recommendations for security plans made under this section shall include protective measures to secure such infrastructure, and milestones and timeframes for implementation.

The Committee recognizes that one of the key purposes of developing a prioritized list of critical infrastructure is to ensure that this infrastructure has adequate security plans. The Committee remains concerned that, in addition to encountering difficulties completing a prioritized list of critical infrastructure, the Department may not be moving quickly enough to assist the owners and operators of critical infrastructure in developing adequate security plans. This section will ensure the Department completes this task within a set time-frame.

Sec. 333. Implementation report

This section directs the Secretary of Homeland Security to report on the implementation of this subtitle no later than 15 months after enactment of this Act, and provide an update one year later.

Sec. 334. Protection of information

This section exempts from disclosure under the Freedom of Information Act information that is generated, compiled, or disseminated by the Department of Homeland Security (Department of DHS) in carrying out this subtitle. If the information covered by this provision is provided to a State or local government, it may not be made available pursuant to any State or local law requiring disclosure of information or records; otherwise be disclosed by a State or local government without written consent of the entity submit-

ting the information; or be used other than to protect critical infrastructure, or to further criminal investigation or prosecution.

Under 6 CFR § 29.8(g), certain information that is related to the security of critical infrastructure that is voluntarily submitted to the Department for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose is treated as exempt from the Freedom of Information Act, and if such information is provided by certain officials in the Department to a State or local government agency, entity or authority, or an employee or contractor thereof, it is protected from any State or local law requiring disclosure of records or information. Section 334 clarifies that similar protections from the Freedom of Information Act and State and local record and information disclosure laws apply to information that is generated, compiled, or disseminated by the Department in carrying out this subtitle.

Certain critical infrastructure information, including information generated, compiled, or disseminated by the Department, may also be designated as classified or protected from public disclosure under existing regulations, and this section is not intended to affect any such other authorities.

TITLE IV—MISCELLANEOUS

Sec. 401. Border security and enforcement coordination and operations

This section requires the Secretary of Homeland Security to review and evaluate the current organizational structure of U.S. Customs and Immigration Enforcement (ICE) and U.S. Customs and Border Protection (CBP), and submit a report of findings and recommendations to the Congress within 30 days of enactment.

Subsection (a) enumerates 12 findings of Congress expressing concern about the organizational, operational, and administrative division of ICE and CBP, and the need for the Secretary's review and report to Congress. These findings are based on oversight conducted by the Committee, including a hearing with current and former ICE and CBP personnel who testified about the problems with the current division of ICE and CBP.

Subsection (b) requires, and specifies, the content of the report, including the following: a description of the rationale for, and any benefits of, the current organizational division of ICE and CBP; an analysis of alternative organizational structures for delivering maximum efficiency and mission success; and recommendations for correcting operational and administrative problems that have been caused by the division of border security and immigration and customs enforcement, including any appropriate reorganization plans.

The Committee is very concerned about the effects of such division on the integrity and effectiveness of our border control system. The Committee understands that the Secretary of Homeland Security is currently undertaking a review that includes, among other things, the proper organization of CBP and ICE, and their component parts. The Committee strongly encourages the Secretary to consider whether a merger of CBP and ICE would help to ensure a more seamless and effective border control system.

The Committee also has been made aware of concerns regarding possible delays in processing by the Bureau of Immigration and Customs Enforcement's Dallas Finance Center of invoices for Federal Protective Service (FPS) contracts. Therefore, the analysis required by this section also should include an assessment of the impact of the current organizational structure on the timeliness of processing invoices for FPS contracts.

The Committee recognizes the challenges presented at the land borders of the United States due to the steadily rising number of commercial vehicles and the Federal and state requirements to conduct homeland security inspections and state safety inspections, respectively. In an effort to help facilitate legitimate trade and travel with Mexico and Canada, the Committee encourages the Department of Homeland Security to consider the feasibility and legal implications of combining, to the extent practicable, state and Federal operations in shared "one-stop" facilities, and to examine the use of new technology systems for the purpose of enhancing homeland security and safety inspections, while expediting transport of people and goods.

It has come to the attention of the Committee that legacy Customs Inspectors and Bureau of Customs and Border Protection (CBP) Officers, who participated in six-day training sessions sponsored by the Federal Law Enforcement Training Center (FLETC) during the period from January 1, 2002 through October 1, 2004, may not have been fully compensated. Concerns have been raised that a number of these Officers and legacy Inspectors may have been entitled to, but not provided, compensation for their sixth day of training each week during their nine- to 12-week training programs. Therefore, the Committee requests that the Commissioner of CBP submit a status report on this issue, including the number of CBP Officers and legacy Customs Inspectors who may be eligible under applicable regulations to back compensation for their sixth training day, the estimated total cost of any back compensation that may be due, and the steps CBP is taking to resolve this issue.

The Committee also has been made aware of concerns regarding possible delays in processing by the Bureau of Immigration and Customs Enforcement's Dallas Finance Center of invoices for Federal Protective Service (FPS) contracts. Therefore, the analysis required by this section also should include an assessment of the impact of the current organizational structure on the timeliness of processing invoices for FPS contracts.

Sec. 402. GAO Report to Congress

Based on its oversight, the Committee recognizes that there are serious management challenges facing the Department, with respect to its organization and chains of command, and with respect to the integration of its many separate legacy agencies into a single, efficient, and effective department. Among these challenges are: (1) the lack of accountability of critical support personnel to the senior operating officers, such as the Chief Information Officer, the Chief Financial Officer, and the Chief Procurement Officer; (2) the lack of consistent and coordinated contract management throughout the Department, particularly involving large, complex, high-cost procurement programs; (3) the challenge of securing the Department's Information Technology infrastructure, and making

it effective for communications and information exchange; and (4) the lack of comprehensive risk assessments to help set priorities and guide department-wide funding and policy strategies.

The Committee supports the 90–day review of the Department of Homeland Security's programs, policies, organization, and operations that was recently initiated by the Secretary. The Committee recognizes, however, that the Congress also has a responsibility to fully examine these management challenges, which—if left unaddressed for too long—could have serious consequences for our national security. Therefore, this section requires the Comptroller General of the United States to submit to Congress not later than six months after enactment of this Act an assessment of the effectiveness of the organizational and management structure of the Department of Homeland Security in meeting its missions, and recommendations on how to address the challenges that remain in achieving a comprehensive management integration strategy for the Department of Homeland Security.

The Committee also notes that it supports the efforts of the Department's Office of the Chief Information Officer and the Directorate for Information Analysis and Infrastructure Protection to create efficiencies through the Department's data center consolidation. The Committee recognizes that interoperability between and among existing data centers remains a challenge, and acknowledges that data centers must be secure, survivable, and able to support continuing operations and continuity of essential government operations in emergency situations. DHS is requested to report back to the Committee with respect to: (1) current plans to enhance, develop, and/or consolidate data centers and data storage facilities; (2) the operational scope of such facilities; (3) details of how DHS plans to implement a fully operational data center back-up function consistent with unclassified continuity of operations standards and classified continuity of government requirements; and (4) how the Office of Management and Budget's data redundancy requirements will be achieved.

Sec. 403. Plan for establishing consolidated and colocated regional offices

The Homeland Security Act of 2002 (HSA) (Public Law 107–296) required the DHS Secretary to develop and submit to Congress a plan for consolidating and co-locating regional and field offices that DHS acquired from its legacy agencies. The HSA required the Secretary to submit this plan not later than one year after enactment of this Act. The Committee notes that this submission was due to Congress by November 2003, and currently is overdue by 17 months.

Therefore, this section requires the Secretary to develop and submit to Congress not later than 60 days after enactment of this Act the plan required by Section 706 of the Homeland Security Act. This plan is essential to enable a rapid, robust, and coordinated Federal response to threats and incidents; provide for integration of capabilities among the Department of Homeland Security, other Federal agencies, and state and local governments; and maximize cost savings and efficiencies through establishment of regional offices at current Department of Homeland Security agency regional

structures with contiguous multi-state operations, wherever appropriate.

Sec. 404. Plan to reduce wait times

This section directs the Secretary of Homeland Security to develop a plan, not later than 180 days after enactment, to improve the operational efficiency of the passenger screening checkpoints to ensure that the average peak time waiting periods do not exceed twenty (20) minutes. It also directs that the Secretary's plan should ensure that no significant disparities exist between immigration and customs processing times among international airports. The Committee has been informed that there are disparities in wait times among international airports in the United States, and there is concern that such disparate wait times will have a long-term economic impact at airports with longer wait times. The Secretary's plan shall also ensure that there is no reduction in security by the measures that may be implemented to eliminate disparities among international airports.

Sec. 405. Denial of transportation security card

Section 70105 of Title 46 of the U.S. Code requires the issuance of Transportation Worker Identification Cards (TWICs) for workers that enter secure areas on vessels or maritime facilities. The Transportation Security Administration (TSA) is currently preparing regulations and testing technologies in advance of fully implementing this requirement.

Section 70105(c)(1) sets out the criteria under which the Secretary can deny a TWIC to an individual, and Section 70105(c)(2) establishes the process under which a waiver of the denial can be obtained. Under paragraph (1) of subsection (c), the Secretary can deny a TWIC to an individual who has been convicted of certain felonies in the preceding seven years, or who otherwise poses a terrorism security risk. Section 405 of this Act clarifies that, when determining if a worker is "otherwise a terrorism security risk," the Secretary can consider felonies that occurred more than seven years before the issuance of the TWIC only if the felony was related to terrorism, as that term is defined in the Homeland Security Act of 2002 (Public Law 107–296).

Section 405 also requires that a hearing under the waiver process established in paragraph (2) be before an Administrative Law Judge. This provision assures that the review of the waiver will be conducted in a separate forum from that in which the determination under paragraph (1) was made.

The Committee recognizes that the TWIC program was developed to address threats and vulnerabilities across all modes of the U.S. transportation system. The Committee is confident that, once implemented, TWIC will ensure the security of passengers, transportation workers, vehicles, and facilities by establishing a system-wide common credential for all personnel requiring unescorted physical or logical access to secure or sensitive areas of the U.S. transportation system. The Committee takes note that, while the initiative is complex, implementation of TWIC has been unnecessarily slow. Therefore, the Committee directs TSA to report to the Committee on the status of the TWIC technology, deployment, and program guidelines within 90 days of enactment.

Sec. 406. Transfer of existing Customs Patrol Officers unit and establishment of new CPO units in the Bureau of Immigration and Customs Enforcement

The "Shadow Wolves" are a specialized unit of Customs Patrol Officers (CPO), created by Congress in 1972, that patrols the international land border within the Tohono O'odham Nation, a sovereign Indian nation, in the State of Arizona. The Shadow Wolves officers are Native Americans who combine modern technology and ancient tracking techniques to identify, pursue, and arrest smugglers along the 76 miles of border and 2.8 million acres within the Tohono O'odham Nation. This unit has proven to be one of the Nation's most valuable assets against narcotics smuggling. Each year, the 21 agents in the Shadow Wolves unit have combined to seize over 100,000 pounds of illegal narcotics.

After the creation of the Department of Homeland Security, the Shadow Wolves unit was transferred to U.S. Customs and Border Protection, and placed under the administrative control of the Tucson Sector of the U.S. Border Patrol. This reorganization has produced uncertainty and a lack of clear direction for the unit, negatively impacting operations and retention of personnel.

This section transfers the Shadow Wolves to U.S. Immigration and Customs Enforcement (ICE), since the unit's work most closely resembles that of ICE Special Agents who investigate and attempt to close down large drug smuggling operations. In addition, this section sets the pay scale of the Shadow Wolves at the same rate as ICE Special Agents.

This section also authorizes new units, similar to the Shadow Wolves, to operate on other similarly situated Indian reservations—such as the Akwesasne (Mohawk) Reservation in upstate New York.

Additional Committee Concerns:

MASS SPECTROMETRY SCREENING TECHNOLOGY

The committee is aware that the Transportation Security Administration (TSA) will have deployed 14 explosive detection trace portals in U.S. airports by May 31, 2005. These portals use a trace detection method called ion mobility spectrometry, which the National Academy of Sciences has found to have limited utility, as they are designed to detect only a specific list of explosives and cannot easily be reconfigured to detect an expanded list of explosives, or chemical and biological threat substances. The National Academy of Sciences has recommended the use of mass spectrometry to improve upon these existing explosive trace detection systems. Based on the National Academy's research, and the recommendation of the 9/11 Commission that this Committee give priority attention to improving the ability of screening checkpoints to detect explosives on aviation passengers, the Committee is supportive of the use of mass spectrometry technology for passenger screening purposes. The Committee, therefore, encourages TSA to continue to develop and deploy mass spectrometry screening portal technology.

PREPARATION FOR 2010 OLYMPIC WINTER GAMES

The Committee understands that the 2010 Olympic Winter Games will be conducted in Vancouver, British Columbia, from February 12 through February 28, and the 2010 Paralympic Winter Games from March 12 through March 21 of that same year. The Committee anticipates that these events of international significance will greatly increase the amount of people and goods crossing the border between Washington State and Canada. The Committee directs the Department of Homeland Security to conduct a review, in conjunction with appropriate Washington State and Canadian entities, and to report back to the Committee on Homeland Security within one year, of all relevant Departmental issues related to the Vancouver Olympic and Paralympic Games, including, but not limited to, expected increases in border flow, necessary enhancements to border security, estimated border crossing wait times, and any need for increased border personnel to be deployed during those times.

BORDER COMMUNICATIONS

The Committee recognizes that mobile communications coverage does not exist in much of the remote areas along the U.S. border with Mexico. This lack of coverage prevents the local residents who observe illegal border activity from rapidly and reliably communicating with the United States Border Patrol. Accordingly, the Department of Homeland Security should work with appropriate entities to improve mobile communications coverage in remote areas along the border. Enhancing communication capabilities will greatly enhance the ability of the Border Patrol to detect and apprehend unknown persons attempting to illegally enter the United States.

IDENT/IAFIS INTEROPERABILITY

The report that accompanied the Fiscal Year 2005 Department of Homeland Security Appropriations Act (PL 108–334) contained language directing the Department to report, by January 16, 2005, on the status of the effort to ensure operational interoperability of the database systems known as IDENT—an immigration-related database—and IAFIS (Integrated Automoated Fingerprint Identification System)—an FBI criminal database. Both of these databases contain biometric information on law violators, and are used by border security officials in screening entrants into the United States. The report is supposed to include an estimate of funds needed and a timetable for full interoperability. The Committee understands that this report has not yet been completed. The Committee is deeply concerned about the progress of the Department in achieving full interoperability between these systems, and directs the Department to report back to the Committee on the status of this effort within 60 days of enactment.

IMPROVING BORDER MANAGEMENT AND IMMIGRATION SECURITY

The Committee notes that the US-VISIT office within the Department of Homeland Security is currently moving towards a comprehensive border management system that utilizes the most current technology available to greatly enhance our homeland secu-

rity. The Committee further notes that, currently, immigration applications and records of immigrant and non-immigrant entries and exits into and out of the United States are largely in paper form. There is no way to access the forms quickly and easily to coordinate events encountered by various bureaus in charge of immigration. A visitor arriving at an airport may have an application for admission that had previously been denied for security reasons just a day or two before. The immigrant may immediately try to enter the United States through a different procedure, but U.S. Customs and Border Protection personnel at a port of entry will have no immediate access to the information suggesting that the immigrant should not be admitted. The Committee wishes to stress the urgent security need for the Department to move as quickly as possible to complete this border management system.

To this end, the Committee stresses the need for the Secretary in the next six months, in consultation with the National Institute of Standards and Technology (NIST) and other appropriate agencies, to examine and analyze all biometric identifiers that have been or might be collected in the future as part of the integrated entry and exit data system required under section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1365a), to conduct background checks with Federal intelligence agencies, to check non-immigrant and immigrant applicants against terrorist or other watch lists, and for purposes of processing and adjudicating applications and petitions for immigration benefits. In this examination and analysis, the Secretary, in consultation with NIST, should consider such factors as accuracy, currently available technology, and the potential for new technology in the future, as well as economic considerations, storage capabilities, efficiency, and feasibility. Based on this study, the Secretary should set appropriate biometric standards for Department-wide immigration and border management purposes.

The Committee also notes the urgent security need for the Department to have instantaneous access to all files on immigrant and non-immigrant applicants for admission into the United States through organized and digital or electronic means. To satisfy this need, the Committee stresses that, in the next six months, the Secretary should analyze and examine options to improve security by establishing a plan to have instantaneous digital access to all Department of Homeland Security immigrant and non-immigrant files, all actions taken by various agencies that come into contact with immigrants and non-immigrants, and any other information necessary to securely and accurately decide whether to admit an immigrant or non-immigrant into the United States. This analysis and examination should consider costs, data security, data privacy, and the ability for immigrants and non-immigrants to correct information stored in their digital files.

Further, the Committee believes there is a need for an analysis and plan on the most accurate and efficient way to organize and access all files on immigrant and non-immigrant applicants and petitioners. The Secretary, in the next six months, should examine and analyze whether all immigrant or non-immigrant files should be registered or catalogued by the receiving agency using a biometric identifier. The Secretary, in consultation with NIST and other

appropriate agencies, should choose one or more alternative biometric identifiers to be used for such purposes.

The Committee also wishes to stress the security need for the Department to have instantaneous digital access to the entry and exit history of all immigrants and non-immigrants seeking admission at a port of entry. To satisfy this need, the Secretary, in the next six months, should analyze and consider replacing Department of Homeland Security paper Form Number I–94 (Arrival/Departure Record) and Form Number I–94W (NIV Waiver Arrival/Departure Record) with procedures that ensure that the functions served by such forms are being carried out by electronic or digitized means. In examining this matter, the Secretary should consider the costs and savings to the Federal government of such replacement, the ability for immigrants or non-immigrants to correct information stored in their digital files, and whether there are any other reasons, including law enforcement or investigative reasons, to maintain paper forms as an additional source of such information.

DHS COMPLIANCE WITH LAW ENFORCEMENT OFFICERS SAFETY ACT

In order to fully comply with the Law Enforcement Officers Safety Act of 2004 (Public Law 108–277), the Secretary of Homeland Security is directed to issue guidelines to its component agencies to which the Act would apply. Such guidelines should include, among other things, a determination of the current, retired, and legacy employees who meet the definition of "law enforcement officer" as applied under the Act. The Department shall report back to the Committee within 180 days after enactment of this Act regarding the issuance of such guidelines and the Department's plans for implementing them.

DHS COMPLIANCE WITH LAW ENFORCEMENT OFFICERS SAFETY ACT

In order to fully comply with the Law Enforcement Officers Safety Act of 2004 (Public Law 108–277), the Secretary of Homeland Security is directed to issue guidelines to its component agencies to which the Act would apply. Such guidelines should include, among other things, a determination of the current, retired, and legacy employees who meet the definition of "law enforcement officer" as applied under the Act. The Department shall report back to the Committee within 180 days after enactment of this Act regarding the issuance of such guidelines and the Department's plans for implementing them.

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) * * *

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

SEC. 2. DEFINITIONS.

In this Act, the following definitions apply:

(1) * * *

* * * * * * *

(17)(A) The term "cybersecurity" means the prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

(B) In this paragraph—

(i) each of the terms "damage" and "computer" has the meaning that term has in section 1030 of title 18, United States Code; and

(ii) each of the terms "electronic communications system", "electronic communication service", "wire communication", and "electronic communication" has the meaning that term has in section 2510 of title 18, United States Code.

* * * * * * *

TITLE I—DEPARTMENT OF HOMELAND SECURITY

* * * * * * *

SEC. 102. SECRETARY; FUNCTIONS.

(a) * * *

* * * * * * *

(e) PARTICIPATION IN FOREIGN COLLECTION REQUIREMENTS AND MANAGEMENT PROCESSES.—The Secretary shall be a member of any Federal Government interagency board, established by Executive order or any other binding interagency directive, that is responsible for establishing foreign collection information requirements and priorities for estimative analysis.

[(e)**]** *(f)* ISSUANCE OF REGULATIONS.—The issuance of regulations by the Secretary shall be governed by the provisions of chapter 5 of title 5, United States Code, except as specifically provided in this Act, in laws granting regulatory authorities that are transferred by this Act, and in laws enacted after the date of enactment of this Act.

[(f)**]** *(g)* SPECIAL ASSISTANT TO THE SECRETARY.—The Secretary shall appoint a Special Assistant to the Secretary who shall be responsible for—

(1) * * *

* * * * * * *

[(g)**]** *(h)* STANDARDS POLICY.—All standards activities of the Department shall be conducted in accordance with section 12(d) of the National Technology Transfer Advancement Act of 1995 (15 U.S.C. 272 note) and Office of Management and Budget Circular A–119.

* * * * * * *

SEC. 104. AUTHORITY FOR DISSEMINATING HOMELAND SECURITY INFORMATION.

(a) PRIMARY AUTHORITY.—Except as provided in subsection (b), the Secretary shall be the executive branch official responsible for disseminating homeland security information to State and local government and tribal officials and the private sector.

(b) PRIOR APPROVAL REQUIRED.—No Federal official may disseminate any homeland security information, as defined in section 892(f)(1), to State, local, tribal, or private sector officials without the Secretary's prior approval, except—

(1) in exigent circumstances under which it is essential that the information be communicated immediately; or

(2) when such information is issued to State, local, or tribal law enforcement officials for the purpose of assisting them in any aspect of the administration of criminal justice.

SEC. 105. HOMELAND SECURITY INFORMATION REQUIREMENTS BOARD.

(a) ESTABLISHMENT OF BOARD.—There is established an interagency Homeland Security Information Requirements Board (hereinafter in this section referred to as the "Information Requirements Board").

(b) MEMBERSHIP.—The following officials are members of the Information Requirements Board:

(1) The Secretary of Homeland Security, who shall serve as the Chairman of the Information Requirements Board.
(2) The Attorney General.
(3) The Secretary of Commerce.
(4) The Secretary of the Treasury.
(5) The Secretary of Defense.
(6) The Secretary of Energy.
(7) The Secretary of State.
(8) The Secretary of the Interior.
(9) The Director of National Intelligence.
(10) The Director of the Federal Bureau of Investigation.
(11) The Director of the National Counterterrorism Center.
(12) The Chief Privacy Officer of the Department of Homeland Security.

(c) FUNCTIONS.—

(1) OVERSIGHT OF HOMELAND SECURITY REQUIREMENTS.—The Information Requirements Board shall oversee the process for establishing homeland security requirements and collection management for all terrorism-related information and all other homeland security information (as defined in section 892(f)(1)) collected within the United States.

(2) DETERMINATION OF COLLECTION PRIORITIES.—The Information Requirements Board shall—

(A) determine the domestic information collection requirements for information relevant to the homeland security mission; and

(B) prioritize the collection and use of such information.

(3) COORDINATION OF COLLECTION REQUIREMENTS AND MANAGEMENT ACTIVITIES.—

(A) COORDINATION WITH COUNTERPART AGENCIES.—The Chairman shall ensure that the Information Requirements Board carries out its activities in a manner that is fully coordinated with the Board's counterpart entities.

(B) PARTICIPATION OF COUNTERPART ENTITIES.—The Chairman and the Director of National Intelligence shall ensure that each counterpart entity—

(i) has at least one representative on the Information Requirement Board and on every subcomponent of the Board; and

(ii) meets jointly with the Information Requirements Board (and, as appropriate, with any subcomponent of the Board) as often as the Chairman and the Director of National Intelligence determine appropriate.

(C) COUNTERPART ENTITY DEFINED.—In this section, the term "counterpart entity" means an entity of the Federal Government that is responsible for foreign intelligence collection requirements and management.

(d) MEETINGS.—

(1) IN GENERAL.—The Information Requirements Board shall meet regularly at such times and places as its Chairman may direct.

(2) INVITED REPRESENTATIVES.—The Chairman may invite representatives of Federal agencies not specified in subsection (b) to attend meetings of the Information Requirements Board.

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) * * *

(b) ASSISTANT SECRETARY FOR INFORMATION ANALYSIS; ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION.—

(1) * * *

* * * * * * *

(4) ASSIGNMENT OF SPECIFIC FUNCTIONS.—The Under Secretary for Information Analysis and Infrastructure Protection—

(A) shall assign to the Assistant Secretary for Information Analysis the responsibility for performing the functions described in paragraphs (1), (4), (7) through (14), (16), and (18) of subsection (d);

(B) shall assign to the Assistant Secretary for Infrastructure Protection the responsibility for performing the functions described in paragraphs (2), (5), and (6) of subsection (d);

(C) shall ensure that the Assistant Secretary for Information Analysis and the Assistant Secretary for Infrastructure Protection both perform the functions described in paragraphs (3), (15), (17), and (19) of subsection (d);

(D) may assign to each such Assistant Secretary such other duties relating to such responsibilities as the Under Secretary may provide;

(E) shall direct each such Assistant Secretary to coordinate with Federal, State, and local law enforcement agencies, and with tribal and private sector entities, as appropriate; and

(F) shall direct the Assistant Secretary for Information Analysis to coordinate with elements of the intelligence community, as appropriate.

* * * * * * *

(d) 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 shall be as follows:

(1) * * *

* * * * * * *

(7) To administer the Homeland Security Advisory System *under section 205*, including—

(A) * * *

* * * * * * *

(20) To require, in consultation with the Assistant Secretary for Infrastructure Protection, the creation and routine dissemi-

nation of analytic reports and products designed to provide timely and accurate information that has specific relevance to each of the Nation's critical infrastructure sectors (as identified in the national infrastructure protection plan issued under paragraph (5)), to private sector officials in each such sector who are responsible for protecting institutions within that sector from potential acts of terrorism and for mitigating the potential consequences of any such act.

(21) To ensure sufficient analytic expertise within the Office of Information Analysis to create and disseminate, on an ongoing basis, products based on the analysis of homeland security information, as defined in section 892(f)(1), with specific reference to the threat of terrorism involving the use of nuclear weapons and biological agents to inflict mass casualties or other catastrophic consequences on the population or territory of the United States.

(22) To ensure that—

(A) the Assistant Secretary for Information Analysis receives promptly and without request all information obtained by any component of the Department if that information relates, directly or indirectly, to a threat of terrorism involving the potential use of nuclear weapons;

(B) such information is—

(i) integrated and analyzed comprehensively; and

(ii) disseminated in a timely manner, including to appropriately cleared State, local, tribal, and private sector officials; and

(C) such information is used to determine what requests the Department should submit for collection of additional information relating to that threat.

(23) To ensure that the Assistant Secretary for Information Analysis—

(A) is routinely and without request given prompt access to all terrorism-related information collected by or otherwise in the possession of any component of the Department, including all homeland security information (as that term is defined in section 892(f)(1)); and

(B) to the extent technologically feasible has direct access to all databases of any component of the Department that may contain such information.

(24) To administer the homeland security information network, including—

(A) exercising primary responsibility for establishing a secure nationwide real-time homeland security information sharing network for Federal, State, and local government agencies and authorities, tribal officials, the private sector, and other governmental and private entities involved in receiving, analyzing, and distributing information related to threats to homeland security;

(B) ensuring that the information sharing systems, developed in connection with the network established under subparagraph (A), are utilized and are compatible with, to the greatest extent practicable, Federal, State, and local government, tribal, and private sector antiterrorism systems and protocols that have been or are being developed; and

(C) ensuring, to the greatest extent possible, that the homeland security information network and information systems are integrated and interoperable with existing private sector technologies.

(25) To ensure that, whenever possible—

(A) the Assistant Secretary for Information 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 Assistant Secretary for Information Analysis produces and disseminates in a classified format.

* * * * * * *

SEC. 203. ALTERNATIVE ANALYSIS OF HOMELAND SECURITY INFORMATION.

The Secretary shall establish a process and assign an individual or entity the responsibility to ensure that, as appropriate, elements of the Department conduct alternative analysis (commonly referred to as "red-team analysis") of homeland security information, as that term is defined in section 892(f)(1), that relates to potential acts of terrorism involving the use of nuclear weapons or biological agents to inflict mass casualties or other catastrophic consequences on the population or territory of the United States.

SEC. 204. 9/11 MEMORIAL HOMELAND SECURITY FELLOWS PROGRAM.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Secretary shall establish a fellowship program in accordance with this section for the purpose of bringing State, local, tribal, and private sector officials to participate in the work of the Homeland Security Operations Center in order to become familiar with—

(A) the mission and capabilities of that Center; and

(B) the role, programs, products, and personnel of the Office of Information Analysis, the Office of Infrastructure Protection, and other elements of the Department responsible for the integration, analysis, and dissemination of homeland security information, as defined in section 892(f)(1).

(2) PROGRAM NAME.—The program under this section shall be known as the 9/11 Memorial Homeland Security Fellows Program.

(b) ELIGIBILITY.—In order to be eligible for selection as a fellow under the program, an individual must—

(1) have homeland security-related responsibilities; and

(2) possess an appropriate national security clearance.

(c) LIMITATIONS.—The Secretary—

(1) may conduct up to 4 iterations of the program each year, each of which shall be 90 days in duration; and

(2) shall ensure that the number of fellows selected for each iteration does not impede the activities of the Center.

(d) CONDITION.—As a condition of selecting an individual as a fellow under the program, the Secretary shall require that the indi-

vidual's employer agree to continue to pay the individual's salary and benefits during the period of the fellowship.

(e) STIPEND.—During the period of the fellowship of an individual under the program, the Secretary shall, subject to the availability of appropriations—

(1) provide to the individual a stipend to cover the individual's reasonable living expenses during the period of the fellowship; and

(2) reimburse the individual for round-trip, economy fare travel to and from the individual's place of residence twice each month.

SEC. 205. HOMELAND SECURITY ADVISORY SYSTEM.

(a) REQUIREMENT.—The Under Secretary for Information Analysis and Infrastructure Protection 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, under the System—

(1) shall include, in each advisory and alert regarding a threat, information on appropriate protective measures and countermeasures that may be taken in response to the threat;

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

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

SEC. 206. FULL AND EFFICIENT USE OF OPEN-SOURCE INFORMATION.

The Under Secretary shall ensure that, in meeting their analytic responsibilities under section 201(d) and in formulating requirements for collection of additional information, the Assistant Secretary for Information Analysis and the Assistant Secretary for Infrastructure Protection make full and efficient use of open-source information wherever possible.

SEC. 207. ASSISTANT SECRETARY FOR CYBERSECURITY.

(a) IN GENERAL.—There shall be in the Directorate for Information Analysis and Infrastructure Protection a National Cybersecurity Office headed by an Assistant Secretary for Cybersecurity (in this section referred to as the "Assistant Secretary"), who shall assist the Secretary in promoting cybersecurity for the Nation.

(b) GENERAL AUTHORITY.—The Assistant Secretary, subject to the direction and control of the Secretary, shall have primary authority within the Department for all cybersecurity-related critical infrastructure protection programs of the Department, including with respect to policy formulation and program management.

(c) RESPONSIBILITIES.—The responsibilities of the Assistant Secretary 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; and

(ii) aid in the detection and warning of attacks on, and in the restoration of, cybersecurity infrastructure in the aftermath of such attacks;

(B) a national cybersecurity threat and vulnerability reduction program that identifies cybersecurity vulnerabilities that would have a national effect on critical infrastructure, performs vulnerability assessments on information technologies, and coordinates the mitigation of such vulnerabilities;

(C) a national cybersecurity awareness and training program that promotes cybersecurity awareness among the public and the private sectors and promotes cybersecurity training and education programs;

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

(E) a national security and international cybersecurity cooperation program to help foster Federal efforts to enhance international cybersecurity awareness and cooperation.

(2) To coordinate with 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 other directorates and offices within the Department on the cybersecurity aspects of their missions.

(4) To coordinate with the Under Secretary for Emergency Preparedness and Response to ensure that the National Response Plan developed pursuant to section 502(6) of the Homeland Security Act of 2002 (6 U.S.C. 312(6)) includes appropriate measures for the recovery of the cybersecurity elements of critical infrastructure.

(5) To develop processes for information sharing with the private sector, consistent with section 214, that—

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

(B) consider roles of Federal, State, local, and foreign governments and the private sector, including the insurance industry and auditors.

(6) 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.

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

(8) To consult with the Office for Domestic Preparedness to ensure that realistic cybersecurity scenarios are incorporated into tabletop and recovery exercises.

(9) To consult and coordinate, as appropriate, with other Federal agencies on cybersecurity-related programs, policies, and operations.

(10) To consult and coordinate within the Department and, where appropriate, with other relevant Federal agencies, on security of digital control systems, such as Supervisory Control and Data Acquisition (SCADA) systems.

(d) AUTHORITY OVER THE NATIONAL COMMUNICATIONS SYSTEM.—The Assistant Secretary shall have primary authority within the Department over the National Communications System.

* * * * * * *

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

SEC. 313. TECHNOLOGY CLEARINGHOUSE TO ENCOURAGE AND SUPPORT INNOVATIVE SOLUTIONS TO ENHANCE HOMELAND SECURITY.

(a) * * *

(b) ELEMENTS OF PROGRAM.—The program described in subsection (a) shall include the following components:

(1) * * *

* * * * * * *

(6) The establishment of a homeland security technology transfer program to facilitate the identification, modification, and commercialization of technology and equipment for use by Federal, State, and local governmental agencies, emergency response providers, and the private sector to prevent, prepare for, or respond to acts of terrorism.

(c) TECHNOLOGY TRANSFER PROGRAM.—In developing the program described in subsection (b)(6), the Secretary, acting through the Under Secretary for Science and Technology, shall—

(1) in consultation with the other Under Secretaries of the Department and the Director of the Office for Domestic Preparedness, on an ongoing basis—

(A) conduct surveys and reviews of available appropriate technologies that have been, or are in the process of being developed, tested, evaluated, or demonstrated by the Department, other Federal agencies, or the private sector or foreign governments and international organizations and that may be useful in assisting Federal, State, and local governmental agencies, emergency response providers, or the private sector to prevent, prepare for, or respond to acts of terrorism;

(B) conduct or support research, development, tests, and evaluations, as appropriate of technologies identified under subparagraph (A), including any necessary modifications to such technologies for antiterrorism use;

(C) communicate to Federal, State, and local governmental agencies, emergency response providers, or the private sector the availability of such technologies for antiterrorism use, as well as the technology's specifications,

satisfaction of appropriate standards, and the appropriate grants available from the Department to purchase such technologies;

(D) coordinate the selection and administration of all technology transfer activities of the Science and Technology Directorate, including projects and grants awarded to the private sector and academia; and

(E) identify priorities based on current risk assessments within the Department of Homeland Security for identifying, researching, developing, testing, evaluating, modifying, and fielding existing technologies for antiterrorism purposes;

(2) in support of the activities described in paragraph (1)—

(A) consult with Federal, State, and local emergency response providers;

(B) consult with government agencies and nationally recognized standards development organizations as appropriate;

(C) enter into agreements and coordinate with other Federal agencies, foreign governments, and national and international organizations as the Secretary determines appropriate, in order to maximize the effectiveness of such technologies or to facilitate commercialization of such technologies; and

(D) consult with existing technology transfer programs and Federal and State training centers that research, develop, test, evaluate, and transfer military and other technologies for use by emergency response providers; and

(3) establish a working group in coordination with the Secretary of Defense to advise and assist the technology clearinghouse in the identification of military technologies that are in the process of being developed, or are developed, by the Department of Defense or the private sector, which may include—

(A) representatives from the Department of Defense or retired military officers;

(B) nongovernmental organizations or private companies that are engaged in the research, development, testing, or evaluation of related technologies or that have demonstrated prior experience and success in searching for and identifying technologies for Federal agencies;

(C) Federal, State, and local emergency response providers; and

(D) to the extent the Secretary considers appropriate, other organizations, other interested Federal, State, and local agencies, and other interested persons.

[(c)] *(d)* MISCELLANEOUS PROVISIONS.—

(1) * * *

* * * * * * *

TITLE IV—DIRECTORATE OF BORDER AND TRANSPORTATION SECURITY

* * * * * * *

Subtitle C—Miscellaneous Provisions

* * * * * * *

SEC. 430. OFFICE FOR DOMESTIC PREPAREDNESS.

(a) * * *

* * * * * * *

(c) RESPONSIBILITIES.—The Office for Domestic Preparedness shall have the primary responsibility within the executive branch of Government for the preparedness of the United States for acts of terrorism, including—

(1) * * *

* * * * * * *

(8) those elements of the Office of National Preparedness of the Federal Emergency Management Agency which relate to terrorism, which shall be consolidated within the Department in the Office for Domestic Preparedness established under this section; **[**and**]**

(9) helping to ensure the acquisition of interoperable communication technology by State and local governments and emergency response providers**[**.**]***; and*

(10) designing, developing, performing, and evaluating exercises at the national, State, territorial, regional, local, and tribal levels of government that incorporate government officials, emergency response providers, public safety agencies, the private sector, international governments and organizations, and other appropriate entities to test the Nation's capability to prevent, prepare for, respond to, and recover from threatened or actual acts of terrorism.

* * * * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * * * *

Subtitle J—Terrorism Preparedness Exercises

SEC. 899a. NATIONAL TERRORISM EXERCISE PROGRAM.

(a) IN GENERAL.—The Secretary, through the Office for Domestic Preparedness, shall establish a National Terrorism Exercise Program for the purpose of testing and evaluating the Nation's capabilities to prevent, prepare for, respond to, and recover from threatened or actual acts of terrorism that—

(1) enhances coordination for terrorism preparedness between all levels of government, emergency response providers, international governments and organizations, and the private sector;

(2) is—

(A) multidisciplinary in nature, including, as appropriate, information analysis and cybersecurity components;

(B) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(C) carried out with the minimum degree of notice to involved parties regarding the timing and details of such exercises, consistent with safety considerations;

(D) evaluated against performance measures and followed by corrective action to solve identified deficiencies; and

(E) assessed to learn best practices, which shall be shared with appropriate Federal, State, territorial, regional, local, and tribal personnel, authorities, and training institutions for emergency response providers; and

(3) assists State, territorial, local, and tribal governments with the design, implementation, and evaluation of exercises that—

(A) conform to the requirements of paragraph (2); and

(B) are consistent with any applicable State homeland security strategy or plan.

(b) NATIONAL LEVEL EXERCISES.—The Secretary, through the National Terrorism Exercise Program, shall perform on a periodic basis national terrorism preparedness exercises for the purposes of—

(1) involving top officials from Federal, State, territorial, local, tribal, and international governments, as the Secretary considers appropriate;

(2) testing and evaluating the Nation's capability to detect, disrupt, and prevent threatened or actual catastrophic acts of terrorism, especially those involving weapons of mass destruction; and

(3) testing and evaluating the Nation's readiness to respond to and recover from catastrophic acts of terrorism, especially those involving weapons of mass destruction.

(c) CONSULTATION WITH FIRST RESPONDERS.—In implementing the responsibilities described in subsections (a) and (b), the Secretary shall consult with a geographic (including urban and rural) and substantive cross section of governmental and nongovernmental first responder disciplines, including as appropriate—

(1) Federal, State, and local first responder training institutions;

(2) representatives of emergency response providers; and

(3) State and local officials with an expertise in terrorism preparedness.

* * * * * * *

TITLE 5, UNITED STATES CODE

* * * * * * *

PART III—EMPLOYEES

* * * * * * *

SUBPART I—MISCELLANEOUS

* * * * * * *

CHAPTER 97—DEPARTMENT OF HOMELAND SECURITY

Sec.
9701. Establishment of human resources management system.
9702. Recruitment bonuses.
9703. Reemployed annuitants.
9704. Regulations.

* * * * * * *

§ 9702. Recruitment bonuses

(a) IN GENERAL.—Notwithstanding any provision of chapter 57, the Secretary of Homeland Security, acting through the Under Secretary for Information Analysis and Infrastructure Protection, may pay a bonus to an individual in order to recruit such individual for a position that is primarily responsible for discharging the analytic responsibilities specified in section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) and that—

(1) is within the Directorate for Information Analysis and Infrastructure Protection; and

(2) would be difficult to fill in the absence of such a bonus. In determining which individuals are to receive bonuses under this section, appropriate consideration shall be given to the Directorate's critical need for linguists.

(b) BONUS AMOUNT, FORM, ETC.—

(1) IN GENERAL.—The amount of a bonus under this section shall be determined under regulations of the Secretary of Homeland Security, but may not exceed 50 percent of the annual rate of basic pay of the position involved.

(2) FORM OF PAYMENT.—A bonus under this section shall be paid in the form of a lump-sum payment and shall not be considered to be part of basic pay.

(3) COMPUTATION RULE.—For purposes of paragraph (1), the annual rate of basic pay of a position does not include any comparability payment under section 5304 or any similar authority.

(c) SERVICE AGREEMENTS.—Payment of a bonus under this section shall be contingent upon the employee entering into a written service agreement with the Department of Homeland Security. The agreement shall include—

(1) the period of service the individual shall be required to complete in return for the bonus; and

(2) the conditions under which the agreement may be terminated before the agreed-upon service period has been completed, and the effect of any such termination.

(d) ELIGIBILITY.—A bonus under this section may not be paid to recruit an individual for—

(1) a position to which an individual is appointed by the President, by and with the advice and consent of the Senate;

(2) a position in the Senior Executive Service as a noncareer appointee (as defined under section 3132(a)); or

(3) a position which has been excepted from the competitive service by reason of its confidential, policy-determining, policy-making, or policy-advocating character.

(e) TERMINATION.—The authority to pay bonuses under this section shall terminate on September 30, 2008.

§ 9703. Reemployed annuitants

(a) IN GENERAL.—If an annuitant receiving an annuity from the Civil Service Retirement and Disability Fund becomes employed in a position within the Directorate for Information Analysis and Infrastructure Protection of the Department of Homeland Security, the annuitant's annuity shall continue. An annuitant so reemployed shall not be considered an employee for the purposes of chapter 83 or 84.

(b) TERMINATION.—The exclusion pursuant to this section of the Directorate for Information Analysis and Infrastructure Protection from the reemployed annuitant provisions of chapters 83 and 84 shall terminate 3 years after the date of the enactment of this section, unless extended by the Secretary of Homeland Security. Any such extension shall be for a period of 1 year and shall be renewable.

(c) ANNUITANT DEFINED.—For purposes of this section, the term "annuitant" has the meaning given such term under section 8331 or 8401, whichever is appropriate.

§ 9704. Regulations

The Secretary of Homeland Security, in consultation with the Director of the Office of Personnel Management, may prescribe any regulations necessary to carry out section 9702 or 9703.

* * * * * * *

SECTION 70105 OF TITLE 46, UNITED STATES CODE

§ 70105. Transportation security cards

(a) * * *

* * * * * * *

(c) DETERMINATION OF TERRORISM SECURITY RISK.—(1) * * *

* * * * * * *

(3) The Secretary shall establish an appeals process under this section for individuals found to be ineligible for a transportation security card that includes notice and an opportunity for a hearing *before an administrative law judge*.

* * * * * * *

(5) In making a determination under paragraph (1)(D), the Secretary shall not consider a felony conviction if—

(A) that felony occurred more than 7 years prior to the date of the Secretary's determination; and

(B) the felony was not related to terrorism (as that term is defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)).

* * * * * * *

MINORITY VIEWS

INTRODUCTION

The Committee reported H.R. 1817, the Homeland Security Authorization Act for Fiscal Year 2006, on Wednesday, April 27, 2005. The bill is the first-ever authorization of the Department of Homeland Security by the standing Committee on Homeland Security. Unfortunately, the legislation, as voted out of Committee, is sparse and far from comprehensive. While we agree with the majority of the provisions, the piecemeal and incomplete approach of the legislation will do little to cure the Department of its ills. It may treat the agency's symptoms, but not its many ailments. Even Chairman Cox agreed with this assessment during Committee mark-up, saying in his opening statement, "[t]his authorization bill is by no means as comprehensive as I would have liked."

We appreciate that the Chairman included provisions in H.R. 1817 that help enhance technology at the Department and create an Assistant Secretary for Cybersecurity. The latter is especially relevant as Congresswoman Zoe Lofgren, along with Congressman Mac Thornberry, have advocated this elevation for the nation's cyber czar since the early days of the 108th Congress when they served as Ranking Member and Chairman, respectively, of the Cybersecurity, Science, and Research & Development Subcommittee of the Select Committee on Homeland Security. This provision has almost universally been supported by the private sector and academia. There is no reason to continue to leave cybersecurity as an afterthought in our nation's security efforts.

We also fully support the Manager's amendment offered by Chairman Cox and Ranking Member Thompson. This amendment includes provisions to reform the ineffective color-coded Homeland Security Advisory System, create a 9–11 Memorial Fellows program, and create cybersecurity training programs in institutions of higher learning.

That said, the bill does not address a large number of dangerous security gaps. The bill leaves virtually untouched several key homeland security areas, including the following:

- risks facing critical infrastructures such as chemical and nuclear plants and the energy grid;
- threats to our airplanes and passengers;
- risks to our rail, public transit system, and buses;
- need for first responders to be able to communicate more effectively;
- need for a comprehensive border strategy;
- threat to our food supply;
- protection of privacy, civil rights, and civil liberties;
- protection of our nation against bioterrorism attacks;
- threats to our ports; and

• improvements in management and organization efficiency and oversight.

All these gaps must be met if our nation is to be as secure as it needs to be. A homeland security authorization bill that does not address these issues is incomplete. We presented a substitute bill at mark-up that addressed the issues that H.R. 1817 did, but also provided for the security of America in those areas with the most glaring gaps. When that substitute was rejected by all the Republicans, we offered several amendments on individual security gaps. The Republican majority on the Committee chose to reject the bulk of these amendments as well.

"THE COMPLETE HOMELAND SECURITY ACT"—SUBSTITUTE BILL

The Democratic substitute to H.R. 1817, "The Complete Homeland Security Act," addresses the significant gaps that exist in our nation's homeland security efforts. The substitute provides for a comprehensive border protection plan, mandates the protection of key critical infrastructures, supports the development of new technologies, establishes structural changes at the Department to better organize it, and takes a number of additional steps. The Democratic substitute represents a genuine strategy for ensuring our homeland is protected now.

The Democratic substitute makes the Department of Homeland Security's budget a priority. It funds the discretionary programs of the Department at approximately $41 billion, $6.9 billion above the President's request. Unlike the President's budget, however, no part of these funds will come from taxing airline tickets. This is because raising the government-mandated "fee" to fly is bad for aviation, for consumers, and for our economy.

The Democratic substitute prioritizes funding for local homeland security programs. It provides $6.49 billion for grants to state and local governments, $2.29 billion more than the President's budget, to help acquire the tools needed by law enforcement and first responders on the front-line of preventing and responding to a terrorist attack. Beyond the President's budget, the Democratic substitute provides:

• $80 million to restore funding to the State Homeland Security Grant Program, the primary source of funds used by the states for acquiring the tools needed to prevent and responds to a terrorist attack;

• $500 million to ensure that all first responders can communicate with one another in the event of an emergency;

• $400 million to restore funding to the Law Enforcement Terrorism Prevention program, which is eliminated under the President's budget. This program provides funding to law enforcement agencies to enhance capabilities for detecting, deterring, disrupting, and preventing acts of terrorism;

• $1 billion to provide grants for port, rail, transit and bus security. These funds are badly needed. The Coast Guard estimates that ports alone will need $5.4 billion in new security investments over the next 10 years;

• $10 million to restore funding to the Emergency Management and Performance Grants (EMPG) program, which is cut by six percent in the President's budget. The EMPG program helps states

and local governments strengthen their emergency management capabilities, while addressing issues of national concern;

• $50 million to restore funding to the Metropolitan Medical Response Systems (MMRS) grant program, which is eliminated in the President's budget, and to expand the program. The MMRS program provides grants to ensure that hospital systems in major metropolitan areas are prepared to respond to mass casualties created by a terrorist attack or other emergency;

• $100 million to hire over 1,000 new firefighters nationwide through the SAFER program. The President's budget has no funding for this program; and

• $150 million to restore funding to the FIRE Act grants program, which provides fire departments across the nation with the equipment they need to respond to a terrorist attack or other emergency.

The substitute also ensures that critical research and development at the Department actually happens. It provides $1.8 billion for Science and Technology Directorate programs, including $418 million to fulfill the Intelligence Reform and Terrorism Prevention Act of 2005 (9/11 Act) commitment to aviation security research and development, such as on the next generation of baggage screening technology. The substitute also provided $115 million for research on technologies to counter Man-Portable Air Defense Systems (MANPADS), and broadens the scope of research to include ground-based technologies previously unsupported by DHS. In addition, the substitute provides $35.4 million for new biological countermeasures and technologies to protect American agriculture from terrorist attack.

To ensure that our critical infrastructure is secure, the substitute provides $873 million to improve assessments of the risks to nuclear power plants, chemical facilities, the energy grid, and other critical infrastructure. It also provides for an adequate number of border patrol agents, inspectors and other Federal law enforcement needs by providing $28.4 billion to the Border and Transportation Security Directorate. The substitute also provided funding for immigration processing and other security functions, such as hiring, training, and equipping 2,000 new border agents, as called for in the 9/11 Act.

To assist our first responders, the substitute provides $3.2 billion for Federal emergency preparedness and response programs. This will ensure that the Federal Emergency Management Agency (FEMA) is able to continue its traditional mission of providing assistance during natural disasters.

The substitute also saves money, including $53 million by eliminating the implementation of a new personnel system at the Department that is unworkable and would adversely affect the hard-working career employees at the agency who give their all every day to securing our nation. Rather than penalizing the Department's workers, the Democratic substitute also provides needed funding for the under-staffed and overworked Office of Inspector General by increasing its budget to $200 million and allowing it to hire at least another 500 more investigators and auditors.

The substitute requires the President to complete a report on why his budget request for Fiscal Year 2006 does not fulfill the

homeland security commitments in the 9/11 Act he signed into law in December, 2004. At the time that he signed the legislation into law the President said, "We'll continue to work with Congress to make sure they've got the resources necessary to do their jobs." Despite this statement, President Bush's budget falls far short of funding the provisions in the 9/11 Act. For example, the Act authorized the hiring of 2,000 new border patrol agents, but President Bush's budget only provides enough funding to hire 210 new agents, despite the continued attention being paid to the lack of security on our borders.

The substitute also provides for a number of policy initiatives that are critically needed to secure our nation. When our substitute was rejected by the Republican majority, we offered a number of these initiatives as individual amendments.

ENHANCING ACCOUNTABILITY: ADDRESSING MANAGEMENT CHALLENGES AT THE DEPARTMENT OF HOMELAND SECURITY

We offered a comprehensive management amendment to assist the Department in getting its house in order. It is clear from hearings and oversight conducted by this Committee that the Department's organizational and structural problems need to be addressed. Experts from within the government, private sector, and academia have all raised questions about the Department's structure and the challenges it faces. While many of our Republican colleagues agreed that the Department's organization is flawed, they still chose to vote against this amendment and leave the Department in a disorganized state. We believe this is simply unacceptable.

The amendment would give the Department's Chief Information Officer the authority needed to secure the DHS' information technology and databases against hackers and terrorists. Our amendment provides new resources to the Department's Office of Inspector General to investigate waste, fraud and abuse and help the Department become the agency that Congress envisioned, and that the American people deserve. It would provide the Office of Inspector General with a $200 million budget, allowing the Inspector General to hire another 500 investigators and auditors. In addition, we believe that the Department's employees should have the same collective bargaining and appeals rights that most Federal employees have, as well as minimal guarantees as to compensation as they are transitioned to a new personnel system. Our amendment also gave "whistleblower" protection to DHS employees who come forward to expose security gaps.

This comprehensive amendment also would make other organizational changes such as the establishing co-located DHS regional offices and an Office of Tribal Security, and strengthening of the Department's Privacy Office. While the Majority rejected these provisions, they did agree to address the issue of tribal coordination in the Manager's amendment. We look forward to seeing their language on this issue before determining if their proposal is adequate.

We also believe that the Department needs to be reorganized along better operational lines. While we appreciate Mr. Souder's amendment to combine CBP and ICE into one organization, the

Democrats believe we should wait to make structural changes until the current evaluation by the DHS Office of the Inspector General is completed. Additionally, we are concerned that this particular merger would still leave the Department with disorganized and disparate operational entities. In order for the Department to function effectively, it needs to be organized based on common business functions and lines of business. The quick merger of 22 agencies and subsequent splitting of several is what created the problems that a proposed merger is supposed to solve. There may be functions and operations that certainly should be merged to promote efficiency and security. By the same token, there may be functions and entities that may be executed more effectively if housed in another area of the Department. We should take this opportunity to do it right. The Committee must act to undertake a comprehensive reorganization of the Department to ensure it effectively and efficiently secures the homeland.

EMERGENCY PREPAREDNESS: ENSURING THAT OUR FIRST RESPONDERS HAVE THE RESOURCES AND TOOLS NECESSARY TO PROTECT AMERICA AND THEMSELVES

Democrats presented an emergency preparedness amendment intended to provide greater focus and coordination to emergency preparedness and first responder issues. We sought to provide additional resources for communications interoperability, including additional spectrum and funding to achieve 100 percent interoperability. There was universal agreement from the Committee that additional spectrum is needed for first responders, but jurisdiction remains a problem. The Minority was pleased to support the Majority's proposal to provide additional technical assistance to local governments for communications interoperability. We also supported the creation of a working group for the transition of defense technology to first responder applications.

Democrats also sought to authorize the existing Citizen Corps Program. This crucial program provides guidance and funding to local Citizen Corps Councils to help prepare citizens for any emergency. We were pleased that the Chairman agreed with us that this issue was important and committed to holding a hearing on citizen preparedness. For existing programs, we supported the authorization of the TOPOFF exercise program and the addition of a prevention exercise to the authorization. We also supported the proposal to require coordination with first responders for all future exercises.

However, on the subject of coordination, we were disappointed that we could not come to an agreement on the creation of a single entity to coordinate emergency medical services (EMS) issues within DHS. The Minority strongly supports the creation of an EMS Administration within DHS to ensure that EMS receives adequate homeland security funding. Recent reports by both DHS and outside groups have indicated that EMS providers have only received approximately four percent of homeland security funding. The Minority also supports the concept of the amendment, which was withdrawn, by Mr. Young to merge the preparedness functions of DHS within FEMA. This change would provide greater coordination for preparedness activities and should be explored further.

In the Democratic emergency preparedness amendment, we worked to ensure that two existing grant programs continue as intended. The EMPG Program, which existed before 9/11, has many applications beyond homeland security and is crucial to local emergency management activities. We strongly believe that this grant program should be distributed directly to the state emergency management officials, rather than going through the state homeland security directors. This change would avoid unnecessary delays that are currently taking place. We are pleased the Majority has agreed to provide report language on this subject. We also attempted to authorize the existing Metropolitan Medical Response System (MMRS) program. The MMRS program enables jurisdictions to achieve an enhanced local capability to respond to mass casualty events during the first hours of a response until significant external assistance can arrive.

BIOTERRORISM: PREPARING AND PREVENTING AN ATTACK

Democrats offered an amendment to close four serious gaps in our biopreparedness. Specifically, our amendment (1) lays the foundation for a comprehensive overhaul of the "bug-to-drug" process used to develop new vaccines and medicines; (2) allows DHS to track dangerous biological materials; (3) requires the Government Accountability Office (GAO) to assess whether the Health and Human Services Department (HHS) is effectively administering the Bioshield Act; and (4) requires the Secretary, in consultation with the Director of the National Institutes of Health, to study whether the dilution of the smallpox vaccine in the Strategic National Stockpile would impact the effectiveness of the vaccine. We are disappointed that the amendment was voted down along party lines.

The "bug-to-drug" provision in the Democratic amendment, also known as "The RAPID Cures Act," requires the Secretary to conduct the first-ever comprehensive assessment of the drug and vaccine development process, as well as an assessment of research and technological opportunities and needs. This provision also requests a detailed proposal from DHS, the Department of Defense, and HHS on how to apply Federal resources and work in partnership with the private sector to begin a program to meet the identified needs. We believe this type of analysis is essential to conduct before implementing or overhauling the current system of developing a new medical countermeasure—which typically takes over 14 years and could cost up to $1 billion. If a bioterror attack occurs, we do not have that kind of time to respond. The world's experience with SARS demonstrated that new infectious diseases can emerge and spread far more quickly than our ability to respond, but we are still not able to rapidly produce a vaccine or cure.

The second element of our amendment addresses another critical element of defending against a bioterror attack: knowing the location of dangerous biological materials at all times. Our amendment requires the Secretary to report to Congress on federal and state pathogen controls, including: an inventory of federal and state laws and regulations governing the inventory management, storage, transportation, handling and access to biological warfare agents and other human and zoonotic pathogens; an analysis of inconsistencies and gaps in the application and enforcement of pathogen

control regimes; and recommendations for harmonizing and strengthening pathogen controls. We believe it is critical to track these dangerous materials closely, somewhat similar to the systems we use—or should use—to track nuclear materials because the release of either material can produce the death of thousands or millions of people.

We believe it is also worthwhile to examine whether existing supplies of smallpox vaccine in the National Stockpile could be diluted, to provide treatment to more people, without reducing its effectiveness. If so, this could save limited government funds as well as lives. Smallpox is a disease which kills approximately 30 percent of its victims, and is estimated to have killed between 300 and 500 million people in the twentieth century before the World Health Organization's successful eradication program. Smallpox now only exists in restricted labs throughout the world. Despite its limited availability, the magnitude of destruction resulting from a terror attack involving a smallpox outbreak is enough to make us take this threat seriously. That is why we developed tools to protect our citizens, such as the smallpox vaccine. It is vital that we investigate whether this asset can be leveraged from existing supplies to treat a greater number of people in the event of an outbreak.

The Democrats are further concerned about how aggressively HHS is implementing the BioShield Program. We believe a GAO study and its recommendations are necessary to help to clarify which cabinet department should administer the program. HHS has had a complicated and often contentious relationship with the biopharma industry. In contrast, the Department of Homeland Security appears to be developing a culture that is willing to actively partner with the private sector, and that, perhaps, that can be extended to the biopharma industry. We believe a good working relationship is critical to the success of such an important program as BioShield II which Congress will begin considering shortly. That is why the issue of "who is in charge" is central to all of our homeland security issues.

Finally, we appreciate that the Chairman agreed to include report language that raises concerns about the Biosurveillance Program. We also appreciate his willingness to work with us to craft bipartisan legislation to address many of these concerns. The Biosurveillance Program, established by the President, integrates health data to rapidly recognize and detect dispersal of biological agents in human and animal populations, food, water, agriculture, and the environment. Creating a national bioawareness system will help to identify a biological attack at the earliest possible moment and permit initiation of a robust response to prevent unnecessary loss of life, economic losses, and social disruption. We look forward to working with our Republican colleagues to craft bipartisan legislation to address these shortfalls in the near future.

AGROTERRORISM: PROTECTING OUR FOOD SUPPLY FROM FIELD TO FORK

We are pleased that the Committee adopted our Democratic amendment requiring the Department of Homeland Security to detail to Congress how it will implement recommendations from a recent GAO report entitled, "Homeland Security: Much Is Being Done

To Protect Agriculture From a Terrorist Attack, but Important Challenges Remain." This report evaluated the progress of DHS in implementing the duties assigned under current statutory mandates, Homeland Security Presidential Directive 9 (HSPD–9), and related executive decisions. The GAO report observed some progress made by DHS, but also identified several areas for improvement by DHS. This bill language acknowledges DHS has not fully implemented its responsibilities under HSPD–9, which focuses on the defense of U.S. agriculture and food infrastructures, and holds them accountable for that lack of progress. The Department's role in HSPD–9 is largely to coordinate the efforts of other agencies, but this is a critical role that ensures all of our agroterror efforts work together as seamlessly as possible.

SECURING OUR BORDERS: LAND, AIR, AND SEA

The Democrats believe that the authorization bill does not adequately address the critical issue of land border security. Keeping our borders open to legitimate travel and trade, and closing the door to harmful people and cargo will mean substantial changes at our land borders, and require the right mix of personnel, technology, and new facilities. Securing the 5,525 miles of the northern border with Canada and 1,933 miles of southern border with Mexico is critical to both our national and economic security. According to the Department's own statistics, the Bureau of Customs and Border Protection processes 1.1 million passengers and pedestrians, including 724,192 aliens, 64,432 truck, rail, and sea containers, 2,639 aircraft, 365,079 vehicles and 75,734 merchandise entries in the course of a regular day, making 135 arrests at ports of entry and 3,179 arrests between ports of entry. In the post 9/11 era, security programs must serve the dual purpose of facilitating travel and commerce.

We believe that the Department should develop and implement a Comprehensive Land Border Security Strategy based on threat and vulnerability assessments of our ports of entry and the vast stretches of land between these ports of entry. The Strategy should also include staffing assessments of the Border Patrol and the inspections staff, and an evaluation of infrastructure needs.

Additionally, we wholeheartedly support the use of technology and the expansion of the "American Shield" initiative to address vulnerabilities between the ports of entry. Technology, an important part of the border security solution, does not replace the inspector or the Border Patrol agent. The need for additional Border Patrol resources was highlighted by the "Minutemen Project," a group of volunteers patrolling the Arizona border. While frustration over illegal immigration is understandable, civilian patrols along our national borders, and especially armed patrols, are troubling since they create a great risk of violence. Underscoring the potential for a serious accident, the incidents of violence and the intensity of the attacks on the agents in the Border Patrol's Tucson sector is averaging one assault every two days and, at that pace, it will experience an 80 percent increase this year. As expressed during the mark up of the legislation, there is a need to further examine this issue and we hope to work with the Majority to do so.

Even with the increases the Border Patrol has received over the past three years, from approximately 350 agents to 1,000 agents, the Border Patrol's ability to stop illegal border crossers along the U.S.-Canada border remains limited. It is important to understand that at any point in time 1,000 Border Patrol agents are not monitoring the northern border. Rather, this total number is divided into shifts that provide 24-hours-a-day coverage. T.J. Bonner, president of the National Border Patrol Union indicates that it "takes three shifts to provide 24/7 coverage, and that, coupled with days off, annual and sick leave, training, etc., leaves only about 25 percent of the workforce on duty at any given time." Thus, the number that we currently use for patrolling the northern border is probably more in the area of 250 agents for 5,525 miles—or one agent for every 22 miles of the border. Additionally, many agents are located away from the border transporting and processing the illegal immigrants that they arrest.

Adding to the staffing difficulties, the recent phase of the Arizona Border Control Initiative which began March 30, 2005, has resulted in the diversion of Border Patrol resources. While it is unclear from which areas the personnel and equipment were relocated, we believe that the areas from which resources were pulled are now at greater risk. The urgent need to relocate resources to Arizona simply emphasizes the need to permanently increase staffing and funding overall. Adding to the shortage at our borders, hundreds of the Border Patrol agents have responded to our nation's call and have been called to active duty in the National Guard. For Fiscal Year 2002 through Fiscal Year 2005, 282 Border Patrol agents were deployed—189 have returned from duty. The need to determine appropriate staffing levels for inspectors at the ports of entry is just as critical as it is for Border Patrol agents. The Democrats strongly encourage the Department to examine overall staffing levels.

Lastly, the Democrats believe that the enforcement of our immigration laws is a federal responsibility. We are deeply concerned about the federal government's desire to outsource that problem and the subsequent cost of enforcing immigration law to the state and local law enforcement authorities. The Democrats believe that funding of the Intelligence Reform and Terrorism Prevention Act is a more appropriate and effective way to improve our nation's border security.

The problems outlined are a result of a piecemeal approach to land border security. This is why we called for a Land Border Security strategy. Pending the completion of the comprehensive Land Border Security Strategy and staffing assessment, we support full funding for the border security provisions in the 9/11 Act, which includes the hiring "of not less than 2,000" Border Patrol agents. We believe that in addition to agents, the Border Patrol must have funding for additional support staff, vehicles, training and facilities in which to place their agents. We also support the creation of a Center for Excellence focused on land border security and appreciate the work of Congressmen Reyes, Smith, and McCaul in bringing this idea to the Committee.

We also support Mr. Souder's amendment that addresses key concerns raised by the Shadow Wolves, an elite unit based on the

Tohono O'odham Nation, composed solely of Native Americans of Blackfoot, Cheyenne and Pima tribes, who are known for their ability to track aliens and the drugs they may carry. We understand that for the Shadow Wolves to function effectively they must be able to maintain a close working relationship with Immigration and Customs Enforcement (ICE) investigators, and that this is difficult because they are in Customs and Border Protection (CBP), reporting to the Border Patrol. It is clear to us that this elite unit belongs in ICE and not in CBP—and that these frontline officers have more in common with ICE agents than with Border Patrol agents. That said, in order for the Shadow Wolves to be effective and fully integrated within ICE, the Committee must act to designate them as investigators to better reflect their role in homeland security. We hope we can work with our Republican colleagues to affect his change in the amendment.

SECURING OUR PORTS AND COASTLINES FROM TERRORIST ATTACK

The Democrats offered an amendment that would strengthen port security by improving the validation process for the Customs Trade Partnership Against Terrorism (C–TPAT), requiring the Department to take steps to improve container security, and authorize $400 million for port security grants. We appreciate the Majority's acceptance of the container security provision, but feel that this authorization bill does not fully address the many challenges associated with port security. We fully support C–TPAT because the trade community plays such a large role in port security, but believe that the program lacks accountability. There are currently 5,000 C–TPAT companies that are less likely to have their containers inspected when they arrive in the United States. The fact that only 500 of these have had their security validated by the Department creates a major security threat. This amendment gives C–TPAT members the option of being validated by CBP or by a private company—certified by the Department. This choice could accelerate the validation process. We also believe the port security funding since September 11th has been wholly inadequate. The Administration issued port security regulations that will require ports to spend $5.4 million over ten years. The country's economic security is dependent on open and secure ports. Given that ports have very thin profit margins and will have to invest heavily in infrastructure improvements to stay competitive in the global economy, we believe that the balance of security and commerce requires an increase in port security funding.

SECURING TRAINS AND PUBLIC TRANSIT ACROSS AMERICA

Democrats offered an amendment that authorized $2.8 billion over three years for rail and transit security grants. It also requires grant recipients to submit emergency response plans and training exercises to the Department as a condition for funding, creates a National Transportation Security Center, and requires the Department to partner with industry to develop security best practices and public awareness initiatives. We appreciate the Majority's acceptance of the provisions requiring the development of

best practices and public awareness initiatives, as both will go a long way to improving rail and transit security.

We believe, however, that the Majority largely ignored rail and transit security in this bill. The two attacks that occurred in Madrid and Russia last year highlight the vulnerability of our rail and transit systems to terrorism. According to major transit operators, funding is the primary barrier to improving security. The American Public Transportation Association states that transit operators have $6 billion in long-term security costs; to this point the Bush Administration has distributed $250 million for rail and transit security. State and local governments are doing all they can to assist rail and transit security costs but greater federal assistance will be needed. We believe that the vulnerability of our rail and transit system to attack necessitates the urgent attention of this Administration and Congress to ensure that the 14 million passengers that use mass transit are safe and secure.

SECURING OUR SKIES

Democrats offered an amendment that would increase funding for in-line Explosive Detection Systems (EDS), require personnel that have access to secure areas of airports undergo security screening and background checks, authorize funding for ground based MANPAD research, evaluate communications devices that could be used by flight crews and air marshals, make improvements to the Federal Flight Deck Officer program, and reopen general aviation at Ronald Reagan National Airport. The Majority expressed concerns that we were increasing funding without regards to risk. Specifically, Chairman Cox cited the provision on MANPAD countermeasures, which he felt could lead the Department to spend billions of dollars on a system that may not be necessary. Our provision authorized $5 million more the Administration's request for MANPAD countermeasures research. It also required that research focus on alternative technologies beyond those that are aircraft centered, which are the most expensive, to see if less costly systems are available.

We also believe that more funding is required for the installation of in-line EDS systems to detect explosives items that could be stashed in passenger baggage. The Department's Inspector General issued an unclassified summary of a classified report on screener performance on April 19, 2005 that concluded that screener performance will not improve without upgrades and enhancements in technology. Funding for EDS installation comes from fees assessed to airline passengers. Currently, $250 million is spent on in-line EDS installation, the DeFazio amendment would have increased this amount to $650 million and would have also required the installation of adequate technology at screening checkpoints. We feel that this amendment addresses the recommendations of the 9/11 Commission Report. The Report stated that the Transportation Security Administration (TSA) and Congress must give priority to improving checkpoint screening and that TSA should expedite the installation of in-line baggage screening systems.

TRANSPORTATION WORKER IDENTIFICATION CARD

Democrats support Mr. Young's amendment requiring that transportation workers that are seeking a waiver under section 70105(c)(2) of the Maritime Transportation Security Act and are denied a Transportation Worker Identification Card (TWIC) have their appeal decided by an administrative law judge. The amendment also states that a worker cannot be denied a TWIC for a felony conviction that occurred more than seven years ago, unless it is connected to terrorism, as defined by the Homeland Security Act. This provision helps assure that workers who have kept a clean record for several years are not punished for past mistakes. While some changes in the legislative language will need to occur before the bill reaches the floor, we believe that individuals that have access to secure areas of transportation facilities should undergo a background check.

HARNESSING OUR NATION'S INTELLIGENCE CAPABILITIES

We appreciate the adoption of the amendment offered by Democrats entitled, "Harnessing Intelligence," as amended by the Chairman. We agree with the Republicans' description of this amendment in report language and the purposes it serves.

SECURING OUR CRITICAL INFRASTRUCTURE

We offered an amendment to secure chemical plants, nuclear plants, and the transportation of hazardous material shipments, but this amendment was rejected by the Republican majority. Our amendment authorized the Secretary to:

- require chemical facilities to conduct vulnerability assessments and make related improvements;
- certify that the location and design of a proposed high-risk nuclear facility provided adequate protection for public health and safety if subject to a terrorist attack;
- conduct comprehensive security assessments of nuclear reactors; and
- regulate the transportation of hazardous materials within six months of enactment of the authorization bill.

We are disappointed that our Republican colleagues chose to leave infrastructures unprotected. This is puzzling, especially in light of observations made by the Chairman that chemical plant security is a vitally important issue that must be addressed.

The rejected amendment would also have made the transportation of hazardous materials safer and provided for re-routing of such materials, when a safer route existed. It also would have required a Department evaluation of the location and design of proposed high-risk nuclear facilities for purposes of ensuring adequate protection of public health and safety in the event of a terrorist attack.

We appreciate the Majority's willingness to work with us on the need to include a role for the Department of Homeland Security in the evaluation of security issues surrounding the siting of new Liquefied Natural Gas (LNG) facilities and the expansion of existing LNG terminals. LNG likely will play an increasingly important part in our nation's energy strategy, and it is essential that the se-

curity vulnerabilities of these facilities are thoroughly assessed before siting or expansion decisions are finalized

PROTECTING CYBERSPACE

Democrats strongly support the idea of conducting basic research in the area of cybersecurity, especially within the Science and Technology Directorate at the Department. We believe this is a necessary precursor to developing new tools to increase the security of the Internet and related systems and networks. We further believe that research into the design and roll-out of new infrastructure should occur at all levels of networking and computer use, so that security becomes "invisible" to the end users and, for the system creators, an integrated aspect of system design and management.

The Internet is currently based upon a series of protocols that were conceived for use within military and academic networks and were not designed for today's modern Internet, which is available to almost anyone located anywhere. The old protocols do not contain security controls sufficient to assure the trusted quality of today's global commercial economy. As a result, new protocols and systems are developed, some in high-risk areas such as the intelligence field, without building adequate security into the "backbone" of these systems. This means that security is always an "afterthought," instead of something that forms the basis of the system. With today's ever-changing threats in cyberspace, we cannot afford to rely on outdated security measures. This will continue to be the case without extensive security research and development to design necessary tools, structures and solutions. We accept the Chairman's offer to continue working on a bi-partisan basis with industry to further refine the parameters of the cybersecurity research that must be done.

OPTIMIZING SCREENING CAPABILITIES

We believe that the Department is failing to fully utilize technology to optimize its screening capabilities. The Department should have real-time electronic access to all information needed for its screening operations and digitize all related paper forms. Only after the Department achieves this objective will we be able to fully monitor the true movement of foreign travelers.

We offered an amendment to require the Secretary to report to Congress on the status of efforts to achieve real-time interoperability between the Integrated Automated Fingerprint Identification System and Automated Biometric Identification System databases. The amendment also required the examination of all biometric identifiers and requested recommendations as to which among these identifiers would be most appropriate for all screening functions, and analyze digitizing all arrival/departure forms.

We thank our Republican colleague for agreeing to work with us on report language that would require the Department to achieve these goals.

ENSURING OPPORTUNITY AT THE DEPARTMENT OF HOMELAND

To ensure opportunity at the Department for all Americans, we offered an amendment that would have required the Department to improve participation rates of employees of all races, national origins, genders, and disabilities at all levels. The amendment also required the Department to address obstacles that small business, minority and women-owned businesses face in trying to do business with the Department. Finally, the amendment creates new opportunities for Historically Black Colleges and Universities, Hispanic Serving Institutions and other minority-serving institutions to participate in the Centers of Excellence program.

We are pleased that the Chairman agreed to work with us to develop legislative language on diversity for inclusion in his Manager's amendment. The Chairman also worked with us to develop report language requiring the Department to review, on an ongoing basis, the applicant pool for the Centers of Excellence program to ensure that a diverse cross-section of institutions is represented.

CONCLUSION

As elected officials, we have a duty to do all we can to secure America. As Members of the Committee on Homeland Security, that responsibility is even greater as our leadership has trusted us to provide the guidance and oversight necessary to make the Department of Homeland Security a success. We are sorely disappointed that our Republican colleagues chose to limit this authorization bill to a few issues, rather than taking a comprehensive approach to protecting our nation. The Committee's first authorization bill should have addressed all the glaring gaps in homeland security, as well as the deficiencies our oversight has uncovered at the Department. The legislation voted favorably by the Committee addresses too few issues and is incomplete. We voted in support of the bill because the few provisions that were included were, with limited exceptions, good provisions. We remain concerned that the Committee has given too little guidance to the Department to allow it to set a course that will correct many of the problems it experienced in its first two years of existence.

BENNIE G. THOMPSON,
Ranking Member.
EDWARD J. MARKEY,
Member.
JANE HARMAN,
Member.
NITA M. LOWEY,
Member.
LORETTA SACHEZ,
Ranking Member, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity.
NORMAN D. DICKS,
Member.
PETER A. DEFAZIO,

Member.
ELEANOR HOLMES NORTON,
Member.
ZOE LOFGREN,
Ranking Member, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment.
BILL PASCRELL, Jr.,
Ranking Member, Subcommittee on Emergency Preparedness, Science, and Technology.
BOB ETHERIDGE,
Member.
KENDRICK B. MEEK,
Ranking Member, Subcommittee on Management, Integration, and Oversight.
SHEILA JACKSON-LEE,
Member.
DONNA M. CHRISTENSEN,
Member.
JAMES R. LANGEVIN,
Ranking Member, Subcommittee on Prevention of Nuclear and Biological Attack.

ADDITIONAL VIEWS OF REPRESENTATIVES EDWARD J. MARKEY

More than three and a half years after the September 11th attacks, gaping loopholes in our country's homeland security continue to put Americans at risk of another devastating attack. The Department of Homeland Security's former Inspector General Clark Kent Ervin testified recently before the Committee's Management, Integration, and Oversight Subcommittee that: "Even in the area where the most time, attention, and resources have been invested—aviation security—serious vulnerabilities remain."

One of our most dangerous vulnerabilities is the failure to screen 100 percent of the cargo that is carried on passenger planes and all-cargo aircraft. Every time we fly, we wait in security lines, empty our pockets, remove our shoes, walk through metal detectors, and have our baggage inspected. We do not complain much—after all, we are told that this is required to keep our planes secure—and we accept that. But what many people do not realize is that every time commercial cargo is loaded onto the very same passenger planes or placed on aircraft that transport only cargo, almost none of it is ever inspected at all.

The security risk created by unscreened cargo is not just theoretical: Pan Am Flight 103 was brought down in 1988 over Lockerbie, Scotland by a bomb contained in unscreened baggage, and Air India flight 182 was downed in 1985 off the coast of Ireland by a bomb placed in unscreened luggage.

Uninspected freight on all-cargo carriers also poses a serious danger. Last summer, the 9/11 Commission reported that Al Qaeda operative Zacharias Moussaoui "Worked * * * on * * * terrorist schemes, such as buying four tons of ammonium nitrate for bombs to be planted on cargo planes." Ammonium nitrate is the same chemical compound that Timothy McVeigh used to kill 168 innocent men, women and children at the Murrah Federal Building in Oklahoma City 10 years ago. Less than two years ago, a young man shipped himself undetected aboard a cargo plane from New York to Texas. We were lucky he was just a lonely twenty-something, not a terrorist.

It is long past the time when we should have adopted a policy that subjects cargo on passenger and all-cargo aircraft to the same level of screening that is performed daily on passengers' checked and carry-on luggage.

During Committee consideration of the Department's Fiscal Year 2006 authorization bill I offered an amendment to require the Secretary of Homeland Security to establish and begin implementing a system to inspect all the cargo transported on passenger planes and all-cargo carriers, so that this cargo is subject to the same level of scrutiny as passengers' luggage. The House has voted twice overwhelmingly—by votes of 278 to 146 and 347 to 47—to require 100%

screening of cargo carried on passenger planes. The airline industry and the Bush Administration strenuously objected to the 100 percent screening mandate, and the Senate ultimately dropped it from the final version of the Department's FY04 appropriations bill.

The aviation experts who are this Committee's "eyes and ears"—namely, the pilots and flight attendants who work aboard aircraft every day—support my amendment to screen 100 percent of the cargo transported on passenger planes and all-cargo carriers. The Coalition of Airline Pilots Associations (CAPA), which represents 30,000 pilots at American Airlines, Southwest, AirTran and other airlines, endorses my amendment. Since offering my amendment last year, I addressed the concerns of the Air Line Pilots Association (ALPA) by including all-cargo carriers under the 100% cargo screening mandate and providing for federal appropriations to implement this mandate, and ALPA supports my amendment. The Association of Flight Attendants, with its 46,000 members, supports my amendment.

While last year's appropriations bill for the Department and the 9/11 reform implementation act included funding for cargo screening R&D, additional cargo inspectors, and related provisions, these measures do not go far enough.

TSA currently handles the screening of cargo carried on passenger planes by using a process it calls the "Known Shipper Program." The Known Shipper Program requires only paperwork to be filed, but no screening to be done. Mail and packages weighing less than 16 ounces are not even subject to the paperwork check—they are loaded straight onto the plane without even a perfunctory paper check! When it comes to freight on all-cargo carriers, inspection is the exception, not the rule—only a tiny portion is physically inspected before loading onboard. TSA now requires air carriers to conduct random inspections of cargo that are randomly verified by TSA—but this still results in almost none of the cargo on passenger planes being physically inspected for explosives or other dangerous materials. TSA is unable to inform us of how many cargo inspections are performed by the air carriers because the air carriers do not have to report to TSA the number of cargo inspections they conduct.

Some have argued that the technology to screen 100% of cargo is not available. But there are numerous companies that are currently selling technology that is being used to screen cargo, including American Science and Engineering; L3 Security and Detection Systems; and Raytheon Cargo Screen. Some have argued that 100% screening is not technically feasible. But countries including Israel, the United Kingdom, and the Netherlands routinely screen cargo. Moreover, Logan Airport in Massachusetts, which has been conducting a cargo screening pilot program, reported in February that "100 percent of all air cargo on all types of aircraft is technically possible." Some have argued that the Known Shipper program is enough to assure the security of cargo. The Known Shipper program is dangerously flawed and easily exploited. TSA has admitted that it has not audited most of the so-called known shippers in its database, and packages weighing less than 16 ounces are not even subject to the Known Shipper Program, even though the bomb

that brought down Pan-Am Flight 103 contained less than 16 ounces of explosive!

While my amendment was defeated during mark-up of the authorization bill, I will continue to work to close a dangerous loophole that puts our nation at risk.

EDWARD J. MARKEY.

ADDITIONAL VIEWS OF CONGRESSMAN KENDRICK B. MEEK

Airlines and airports are more than just transportation depots. They are economic engines that employ millions of people, sustain local economies and create many kinds of commercial opportunities. Airlines, especially those serving international passengers, are totally dependent on the federal government for the staffing support and processing of passengers that is required by federal law. They cannot do it themselves. And by failing to provide the needed federal inspection personnel, the federal government itself is putting American businesses—big and small alike—at a huge competitive disadvantage.

The staff shortages in South Florida are instructive. Miami International Airport (MIA) is particularly dependent on federal inspectors. MIA has the most foreign nationals entering our country of any U.S. airport, as well as the most visitors from countries for which the U.S. requires a visa. In addition, MIA continues to have more international transiting passengers—those foreign travelers connecting through MIA from one international destination to another—than any other U.S. airport. These passengers still must be admitted into the U.S. and clear customs before boarding their next flight. Miami is also one the largest cargo airports in the nation, and the majority of arriving goods are perishables requiring agricultural inspections.

However, despite the great and demonstrable need for federal inspection personnel at MIA, Customs and Border Patrol (CBP) is unable to staff the available primary inspection booths during peak international arrival periods—a major contributor to what the federal government's own statistics demonstrate are among the nation's longest wait times for customs and immigration inspections. But MIA is hardly unique. Many major international airports in the U.S. have a shortage of Federal Inspection Service (FIS) officers.

The problem is getting worse. MIA's new South Terminal, which is nearing completion, will have a state-of-the-art FIS facility with 40 primary inspection booths capable of handling 2,000 passengers per hour. This new inspection facility, along with the two already in operation, needs to be fully staffed at peak times to accommodate the thousands of passengers arriving daily. However, despite the fact of present shortages and the predictable need for more, the committee has not acted to address this need.

In addition, smaller airports such as Opa-Locka Airport and Fort Lauderdale Executive Airport have developed growing businesses in private aircraft and executive jet travel, but their growth is limited because of the limited hours of CBP operations.

Instead of addressing these problems, I am concerned that the committee is actually avoiding them. Among the amendments offered to this bill and not supported by the majority was one that

simply required an objective assessment of the adequacy of CBP personnel nationwide. I am hopeful that we can correct this deficiency and address the CBP and Immigration and Customs Enforcement staffing problems as this authorization, bill moves through the legislative process, for this would greatly improve the bill.

KENDRICK B. MEEK.

U.S. House of Representatives
Committee on Agriculture
Room 1301, Longworth House Office Building
Washington, DC 20515-6001
(202) 225-2171
(202) 225-0917 FAX

May 2, 2005

The Honorable Christopher Cox
Chairman, Committee on Homeland Security
U.S. House of Representatives
202 Adams Building, Library of Congress
Washington, D.C. 20515

Dear Chairman Cox:

On April 27, 2005, the Committee on Homeland Security ordered reported a committee print titled the, "Department of Homeland Security Authorization Act for Fiscal Year 2006." Section 309 of the bill, which provides for a report to Congress on protecting agriculture from terrorist attack, falls within the jurisdiction of the Committee on Agriculture. Recognizing your interest in bringing this legislation before the House quickly, the Committee on Agriculture agrees not to seek a sequential referral of the bill. By agreeing not to seek a sequential referral, the Committee does not waive its jurisdiction over this provision or any other provisions of the bill that may fall within its jurisdiction. The Committee also reserves its right to seek conferees on any provisions within its jurisdiction considered in the House-Senate conference, and asks for your support in being accorded such conferees.

Please include this letter as part of the report on the Department of Homeland Security Act for Fiscal Year 2006, or as part of the Congressional Record during consideration of this bill by the House.

Sincerely,

Bob Goodlatte,
Chairman

CHRISTOPHER COX, CALIFORNIA
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Ninth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

May 2, 2005

The Honorable Bob Goodlatte
Chairman
Committee on Agriculture
2120 Rayburn House Office Building
Washington, D.C. 20515

Dear Mr. Chairman:

Thank you for your recent letter expressing the Agriculture Committee's jurisdictional interest in section 309 of the "Department of Homeland Security Authorization Act for Fiscal Year 2006." I appreciate your willingness not to seek a sequential referral in order to expedite proceedings on this legislation. I agree that, by not exercising your right to request a referral, the Agriculture Committee does not waive any jurisdiction it may have over section 309. In addition, I agree to support representation for your Committee during the House-Senate conference on provisions determined to be within your Committee's jurisdiction.

As you have requested, I will include a copy of your letter and this response as part of the Committee on Homeland Security's report for the *Congressional Record* during consideration of the legislation on the House floor. Thank you for your cooperation as we work towards the enactment of the "Department of Homeland Security Authorization Act for Fiscal Year 2006."

Sincerely,

Christopher Cox
Chairman

cc: The Honorable J. Dennis Hastert, Speaker
The Honorable Bennie Thompson, Ranking Member
The Honorable Collin C. Peterson, Ranking Member
The Honorable John Sullivan, Parliamentarian

COMMITTEE ON ARMED SERVICES

U.S. House of Representatives

Washington, DC 20515–6035

ONE HUNDRED NINTH CONGRESS

May 2, 2005

Honorable Christopher Cox
Chairman, Committee on Homeland Security
U.S. House of Representatives
202 Adams Building, Library of Congress
Washington, D.C. 20515

Dear Mr. Chairman:

On April 27, 2005, the Committee on Homeland Security ordered reported a committee print, the "Department of Homeland Security Authorization Act for Fiscal Year 2006." This bill contains provisions that fall within the jurisdiction of the Committee on Armed Services, including: section 222 (relating to information collection requirements and priorities) and section 302(b) (establishing a working group relating to military technology). Recognizing your interest in bringing this legislation before the House quickly, the Committee on Armed Services agrees not to seek a sequential referral of the bill. By agreeing not to seek a sequential referral, the Committee does not waive its jurisdiction over these provisions or any other provisions of the bill that may fall within its jurisdiction. The Committee also reserves its right to seek conferees on any provisions within its jurisdiction considered in the House-Senate conference, and asks for your support in being accorded such conferees.

Please include this letter as part of the report, if any, on the Department of Homeland Security Act for Fiscal Year 2006 or as part of the Congressional Record during consideration of this bill by the House.

Sincerely,

Duncan Hunter
Chairman

DH: hm

CHRISTOPHER COX, CALIFORNIA
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Ninth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

May 2, 2005

The Honorable Duncan Hunter
Chairman
Committee on Armed Services
2120 Rayburn House Office Building
Washington, D.C. 20515

Dear Mr. Chairman:

Thank you for your recent letter expressing the Armed Services Committee's jurisdictional interest in Section 222 and the working group on transfer of military technologies established under Section 302(b) of the "Department of Homeland Security Authorization Act for Fiscal Year 2006." I appreciate your willingness not to seek a sequential referral in order to expedite proceedings on this legislation. I agree that, by not exercising your right to request a referral, the Armed Services Committee does not waive any jurisdiction it may have over the relevant provisions of Sections 222 and 302(b). In addition, I agree to support representation for your Committee during the House-Senate conference on any provisions determined to be within your Committee's jurisdiction.

As you have requested, I will include a copy of your letter and this response as part of the Committee on Homeland Security's report and the *Congressional Record* during consideration of the legislation on the House floor. Thank you for your cooperation as we work towards the enactment of the "Department of Homeland Security Authorization Act for Fiscal Year 2006."

Sincerely,

Christopher Cox
Chairman

cc: The Honorable J. Dennis Hastert, Speaker
The Honorable Bennie Thompson, Ranking Member
The Honorable Ike Skelton, Ranking Member
The Honorable John Sullivan, Parliamentarian

O