109TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 109–71
Part 3

DEPARTMENT OF HOMELAND SECURITY AUTHORIZATION ACT FOR FISCAL YEAR 2006

MAY 13, 2005.—Ordered to be printed

Mr. SENSENBRENNER, from the Committee on the Judiciary, submitted the following

R E P O R T

[To accompany H.R. 1817]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, 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.

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:

SEC. 3. DEFINITIONS.

For purposes of this Act, the terms "prevent terrorist attacks" and "terrorism prevention" are intended to encompass securing our borders, securing our critical infrastructure, disseminating homeland security information to Federal, State, and local government agencies, and preparing first responders for a terrorist attack.

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. IMMIGRATION RESOURCES.

(a) 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.

(b) Of the amount authorized under section 101, there is authorized to be appropriated for fiscal year 2006 for the U.S. Immigration and Customs Enforcement Legal Program sufficient sums for the hiring of an additional 300 attorneys in addition to the number employed on the date of this Act, and related training and support costs.

(c) Of the amount authorized under section 101, there is authorized to be appropriated for fiscal year 2006 for U.S. Citizenship and Immigration Services sufficient sums for the hiring of an additional 300 adjudicators to carry out the functions stated in section 451(b) of the Homeland Security Act of 2002 in addition to the number employed on the date of this Act, and related training and support costs.

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.

(a) FISCAL YEAR 2006.—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);

(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; and

(3) subsequent to the completion of a feasibility study by the Federal Government finding conclusively the need for a regional homeland security center which enhances coordination for terrorism preparedness between all levels of government, sufficient sums as may be necessary for the development of a center for training for Federal, State, and local law enforcement officials with an expertise in terrorism preparedness.

(b) USE OF GRANTS FOR "TERRORISM COPS".—

(1) IN GENERAL.—Notwithstanding any other provision of law, a covered grant may be used to pay the salaries of law enforcement officers hired exclusively for terrorism and homeland security matters.

(2) COVERED GRANT.—In this subsection, the term "covered grant" applies to—

(A) the State Homeland Security Grant Program of the Department, or any successor to such grant program;

(B) the Urban Area Security Initiative of the Department, or any successor to such grant program; and

(C) the Law Enforcement Terrorism Prevention Program of the Department, or any successor to such grant program.

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 and the Committee on the Judiciary of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary 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 of the vulnerabilities in relation to 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.

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

(C) 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.

(D) The policies and procedures the Secretary shall establish to ensure the Department disseminates this information received from the National Counter Terrorism Center throughout the Department, as appropriate; utilizes this information to support the Department's mission to reduce vulnerability to terrorism; integrates the Department's information collection and analysis functions; and disseminates this information to its operational units, as appropriate.

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

(F) A description of initiatives the Secretary shall take to share homeland security information with, and provide homeland security support to, State and local governments and the private sector.

(G) 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.

(H) Such other elements as the Secretary considers appropriate consistent with this plan.

(3) CONSULTATION.—In formulating the Plan to reduce the vulnerability of the United States to terrorist attacks, 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) Intelligence and law enforcement operations that screen for individuals who plan or intend to carry out acts of terrorism.

(B) Intelligence and law enforcement operations that identify and respond to vulnerabilities of the United States to terrorism.

(C) Operations to detect and prevent terrorist attacks within the United States, including 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) Utilization by the Department of Homeland Security of information and intelligence received from other Federal agencies, and foreign, State, local, tribal and private sector officials, to detect or prevent acts of terrorism.

(H) Dissemination by the Department of Homeland Security of information to other Federal agencies, and State, local, tribal and private sector officials.

(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 consult with the Attorney General, to 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.

"The Secretary shall be the principal executive branch official responsible for disseminating homeland security information to State and local government and tribal officials and the private sector. ".

(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 Federal, 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. 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. 223. 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. 224. 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(c)) 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, in concurrence with the Attorney General and the National Director of Intelligence, 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;

"(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 in concurrence with the Attorney General and the National Director of Intelligence 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, includ-

ing 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 and the Committee on the Judiciary of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee

on the Judiciary 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 en-

courage 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, in concurrence with the Attorney General and the National Director of Intelligence 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 and the Committee on the Judiciary of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary 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 the Bureau of 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 U.S. 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 functions, or to combine immigration-related enforcement functions with customs and other functions, contrary to the design of the Bureau of Border Security as prescribed by the Congress in section 442 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) U.S. 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 U.S. Immigration and Customs Enforcement to impose hiring freezes and to release aliens that otherwise should be detained.

(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 U.S. Immigration and Customs Enforcement and the Bureau of 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 the Bureau of Customs and Border Protection and U.S. Immigration and Customs Enforcement, and areas of unnecessary overlap or operational gaps among and between these missions;

(C) a description of the rationale for, and any benefits of, the current organizational combination of immigration-related enforcement functions with customs and other functions;

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

(E) 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;

(F) an analysis of whether the Federal Air Marshals and the Federal Protective Service are properly located within the Department within U.S. Immigration and Customs Enforcement;

(G) 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;

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

(I) recommendations for correcting the operational and administrative problems that have been caused by the division of the Bureau of Customs and Border Protection and U.S. Immigration and Customs Enforcement and by the combination of immigration-related enforcement functions with cus-

toms and other functions in both entities, 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) that an individual poses a terrorism security risk, the Secretary shall not consider, as the sole reason, 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 an offense that is a violation of a provision specified in subparagraph (B) of section 2332b(g)(5) of title 18.".

SEC. 406. TRANSFER OF EXISTING CUSTOMS PATROL OFFICERS UNIT AND ESTABLISHMENT OF NEW CPO UNITS IN THE U.S. 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 U.S. 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 U.S. 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 U.S. 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.

SEC. 407. DATA COLLECTION ON USE OF IMMIGRATION CONSULTANTS.

The Secretary of Homeland Security shall establish procedures to record information on applications for an immigration benefit submitted by an alien with respect to which—

(1) the alien states that the alien used the services of an immigration consultant; or

(2) a Department employee or official investigating facts alleged in the application, or adjudicating the application, suspects that the alien used the services of an immigration consultant.

PURPOSE AND SUMMARY

H.R. 1817, the "Homeland Security Department Authorization Act for Fiscal Year 2006," represents the first legislative authorization of the Department of Homeland Security since it was established after enactment of the Homeland Security Act (Pub. L. No. 107–296).

BACKGROUND AND NEED FOR THE LEGISLATION

The House Committee on the Judiciary played an integral role in creating the Department of Homeland Security ("DHS" or "Department") and retains legislative and oversight jurisdiction over several components within it. In addition, the Committee on the Judiciary has conducted rigorous oversight of the operation of the DHS since its establishment. H.R. 1817 was introduced by Rep. Christopher Cox on April 26, 2005, and reported by the Committee on Homeland Security by voice vote on April 27, 2005. The Judiciary Committee received a sequential referral on the legislation until May 13, 2005. H.R. 1817 makes a number of modifications to the operation of DHS in order to streamline its management and organization.

House Rule X provides the Committee on the Judiciary with jurisdiction over "criminal law enforcement" [1] and "subversive activities affecting the internal security of the United States." [2] As a result, the Committee has jurisdiction over criminal law enforcement activities undertaken by a number of Federal agencies, including law enforcement activities undertaken by DHS. The Committee also has exclusive jurisdiction over the nation's immigration and naturalization laws.[3] As a result, non-border security-related responsibilities of DHS are within the sole jurisdiction of the Committee on the Judiciary.

TERRORISM PREVENTION: DEFINITION AND BACKGROUND

When establishing the Department of Homeland Security, Congress intended to streamline homeland security functions of the Federal government to eliminate mission redundancy and to improve coordination to respond to terrorist attacks. The Homeland Security Act of 2002 indicated that one of the missions of the Department is to "prevent terrorist attacks within the United States." While the same term is used to describe the mission of the Department of Justice, the legislative history surrounding passage of the Homeland Security Act, and subsequent Homeland Security Presidential Directives, demonstrate that there are crucial differences between these missions.

During consideration of the Homeland Security Act, the Committee on the Judiciary expressed concern that this phrase would confuse the Department of Homeland Security's mission with that of the Department of Justice, creating more duplication and uncer-

[1] House Rule X(1)(1)(7).
[2] House Rule X(1)(1)(19).
[3] House Rule X(1)(1)(9).

tainty rather than streamlining the homeland security functions of the Federal Government. As is made clear in H.R. Rep. No. 107–609, which was prepared by the House Select Committee on Homeland Security and accompanied the Homeland Security Act, the prevention of terrorism has a specific definition when used to describe the mission of the Department of Homeland Security. Specifically, the report states: "The Department [of Homeland Security's]s primary responsibilities will include: analyzing information and protecting infrastructure; developing countermeasures against chemical, biological, radiological, and nuclear attacks; securing U.S. borders and transportation systems; organizing emergency preparedness and response efforts; conducting homeland security related research, development, technology, and acquisition programs; coordinating counter-terrorism activities with other Federal agencies, State and local governments, and the private sector."

Homeland Security Presidential Directives (HSPD) issued after the establishment of the Department of Homeland Security further clarify this distinction. Issued in February of 2003, Paragraph (4) of HSPD–5[4] defines the Secretary of Homeland Security as the principal Federal official for domestic incident management. HSPD–5 explains that pursuant to the Homeland Security Act of 2002, the Secretary is responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. HSPD–5 distinguishes this role from the investigative authority to prevent terrorism.

Paragraph (8) of HSPD–5, clearly dictates that it is the Attorney General who "has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at United States citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States, as well as for related intelligence collection activities within the United States, subject to the National Security Act of 1947 and other applicable law, Executive Order 12333, and Attorney General-approved procedures pursuant to that Executive Order. Generally acting through the Federal Bureau of Investigation, the Attorney General, in cooperation with other Federal departments and agencies engaged in activities to protect our national security, shall also coordinate the activities of the other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States. Following a terrorist threat or an actual incident that falls within the criminal jurisdiction of the United States, the full capabilities of the United States shall be dedicated, consistent with United States law and with activities of other Federal departments and agencies to protect our national security, to assisting the Attorney General to identify the perpetrators and bring them to justice."

HSPD–8[5] is a companion to HSPD–5, and further clarifies this critical distinction. Issued in December of 2003, HSPD–8 describes the way Federal departments and agencies will prepare for an attack including prevention activities during the early stages of a terrorism incident. Under HSPD–8, the term "prevention" has a nar-

[4] http://www.whitehouse.gov/news/releases/2003/02/20030228–9.html
[5] http://www.whitehouse.gov/news/releases/2003/12/20031217–6.html

rower meaning than in HSPD–5. HSPD–8 states that the term "prevention" refers to activities undertaken by the first responder community during the early stages of an incident to reduce the likelihood or consequences of threatened or actual terrorist attacks. More general and broader efforts to deter, disrupt, or thwart terrorism are not addressed in this directive [HSPD–8]."

Both types of terrorism prevention require the involvement of law enforcement, and both are vital to the security of our Nation. However, continuing confusion about the distinction between these two prevention missions perpetuates the overlap, duplication, turf battles, and information hoarding that the Homeland Security Act sought to eliminate. Similarly, the Department of Justice should continue to carry out its mission as the primary Federal agency for investigating and prosecuting terrorism. Finally, it is the Committee on the Judiciary's understanding that H.R. 1817 will not alter or diminish the existing authority of Federal agencies (as defined in statute, regulation, or presidential directive, finding or Executive Order) other than the Department of Homeland Security.

IMMIGRATION ENFORCEMENT AT DHS—BACKGROUND, HISTORY, AND PRESENT ISSUES

The transfer of immigration enforcement and services functions from the Immigration & Naturalization Service (INS) to the Department of Homeland Security (DHS), while eliminating a problematic dual mission between immigration service and enforcement, has instead created a similarly conflicting mission between customs and immigration enforcement. Unfortunately, the Department of Homeland Security, Immigration & Customs Enforcement (ICE) and Customs and Border Protection (CBP) both suffer from dual competing missions. Even more problematic, however, are indications that ICE, and to a lesser extent CBP, have been prioritizing customs enforcement over immigration enforcement (the "customization of" ICE and CBP). Furthermore, the leadership of both organizations has been dominated by former U.S. Customs officials.

The Homeland Security Act of 2002 did not establish the present organization of CBP and ICE (to include customs and other enforcement responsibilities). In fact, at no time during reorganization planning was it anticipated by the Committee on the Judiciary or other committees in Congress that an immigration enforcement agency would share its role with other enforcement agencies or that interior immigration enforcement would be separated from border protection. Such dual or even multiple mission agencies were never discussed in any official proceedings in Congress, and, in fact, as noted below, the congressional record indicates the reorganization of INS was intended in large part to avoid the problems inherent in dual missions.

Formation and present organization of CBP and ICE

The Homeland Security Act of 2002 transferred INS' immigration service function to U.S. Citizenship & Immigration Services (USCIS), and enforcement functions to ICE and CBP. To a great extent, ICE and CBP are led by former customs officials and geared towards customs enforcement.

An examination of CBP leadership reveals an emphasis on customs over immigration. Mr. Robert Bonner was head of the Drug Enforcement Agency (DEA), an organization that like the former Bureau of Customs is devoted to anti-drug enforcement (as GAO report GAO–05–81 states, "Customs investigators who specialized in customs enforcement (e.g., drug smuggling)"). The online biography of the Deputy Commissioner of CBP also reveals a heavy customs enforcement background. Presently, all other top leadership positions at CBP have been assigned to persons with customs, rather than immigration enforcement backgrounds. At ICE, a similar phenomenon has occurred except for Assistant Secretary for ICE, Michael Garcia, who was formerly an Assistant U.S. Attorney and briefly the former Commissioner at INS. At the "street level," virtually all of the Special Agents in Charge (SACs) at ICE were assigned from the former Bureau of Customs. This scarcity of individuals with immigration-related backgrounds has undermined the quality of immigration enforcement at both CPB and * * *.

Government Accountability Office report

The Government Accountability Office (GAO) studied the transition of INS into the Department of Homeland Security (DHS) late last year. The creation of USCIS has been relatively smooth (despite the enormous continued presence of an immigration petition backlog and the loss of a credible anti-fraud program). USCIS remains an entity that focuses solely on immigration service. However, GAO concluded that CBP and especially ICE, remain in transition mode:

> CBP brought together INS and Customs inspections programs that, prior to the transition, largely worked side by side in many land ports of entry around the country and that shared similar missions. CIS was a direct transfer of the Immigration Services Division within INS and the program remained largely intact. In contrast ICE is a patchwork of agencies and programs that includes INS's investigations and intelligence programs, Customs' air and marine interdiction division, the Federal Protective Service, and the Federal Air Marshals. * * * The integration of INS and Customs investigators into a single investigative program has involved blending of two vastly different workforces * * * [b]oth programs were in agencies that prior to the merger had differences investigative priorities. Both programs were in agencies with dual missions that prior to the merger differences in investigative priorities.

GAO also identified immigration application fraud as an area of disagreement between USCIS and ICE Field Offices. Apparently, USCIS continues to forward cases to ICE that USCIS believes should be investigated, but ICE declines to investigate a vast majority of those cases, citing limited resources:

> Prior to the transition, INS had begun to place a priority on investigating benefit fraud perpetrated by large scale organizations * * * this has continued under ICE. As a result, some CIS field offices told us that ICE would not pursue single cases of benefit fraud. ICE field officials who spoke on this issue cited a lack of investigative resources.

History of restructuring legislation

Approved by the House by a vote margin of 405–9, the "Barbara Jordan Immigration Reform and Accountability Act of 2002" (H.R. 3231) would have abolished INS and created an Office of Associate Attorney General for Immigrant Affairs within the Department of Justice. Under the newly created Office, two new bureaus would have been established, the Bureau of Citizenship and Immigration Services and the Bureau of Immigration Enforcement. Each Bureau would have been headed by a director who would have reported to the Associate Attorney General for Immigration Affairs. Within each Bureau would have been the following newly created offices and positions: (1) Office of Policy and Strategy; (2) Legal Advisor; (3) Chief Budget Officer; and (4) Office of Congressional Intergovernmental and Public Affairs.

Importantly, the U.S. Commission on Immigration Reform, the commission headed by Barbara Jordan that first proposed breaking up INS, found that:

> the INS does not receive the attention it deserves, given the *importance of immigration policy to our national well-being and security*. Creating the new Associate Attorney General elevates immigration issues within the Justice Department and ensures that immigration will consistently receive the attention, management, and oversight that it needs. (Emphasis added). The Commission also:
>
> recommend[ed] fundamental restructuring of responsibilities within the federal government to support more effective management of the core functions of the immigration system * * * *the immigration system is one of the most complicated* in the federal government bureaucracy * * * one agency has multiple, and sometimes conflicting, operational responsibilities * * * further recommends that the *newly configured agency have the prominence and visibility that the Federal Bureau of Investigation [FBI]* currently enjoys * * * (Emphasis added).

The Bureau of Immigration Enforcement was to be headed by a director who would have a minimum of ten years of law enforcement professional experience, at least five of which must have been in a managerial capacity (it was always anticipated that the agency would only have an immigration enforcement mission, however).

Under the proposed legislation, the newly created Immigration Enforcement Bureau would have been responsible for all border patrol, inspections, detention, removal, investigation, and intelligence functions. The act would have also transferred the enforcement functions of the Office of Special Investigations from DOJ's Criminal Division and the enforcement functions of the Office of Immigration Litigation from DOJ's Civil Division to the newly created bureau.

Homeland Security Act of 2002

Section 441 of the Act transferred all immigration enforcement functions to a newly established "Bureau of Border Security." The legislation specifically only mentions the transfer from INS of "the Border Patrol program, the detention and removal program, the intelligence program, the investigations program, the inspections pro-

gram," and does not mention agriculture of customs enforcement, Federal Air Marshals or Federal Protective Service. (INS' immigration service was ultimately transferred to U.S. Citizenship & Immigration Services (USCIS), and enforcement functions to ICE and CBP. In so doing, former INS Border Patrol was combined with U.S. Customs inspectors from the Department of Treasury, and agricultural inspectors from the Department of Agriculture, to create CBP. ICE was formed from former INS internal enforcement, Treasury anti-money laundering and customs enforcement from the Department of the Treasury, Federal Protective Service, and the Federal Air Marshals.)

The President had the authority pursuant to section 1502(c) of the Act to modify the provisions relating to INS functions in his November 25, 2002, DHS Reorganization plan. The modification only made changes within the Border and Transportation Security Directorate. Under the modified reorganization plan, DHS would bring together the various border agencies into the Bureau of Customs and Border Protection. Specifically, CBP is comprised of the resources and missions relating to borders and ports of entry of the Customs Service, INS's Border Patrol and inspections program, and the U.S. Department of Agriculture's Agricultural Quarantine Inspection program.

ICE was to bring together the interior enforcement and investigation arms of the Customs Service, with INS's detention and removal, intelligence, and investigation programs. The new Bureau of Immigration and Customs (later renamed ICE) would also contain the Federal Protective Service. It was anticipated that ICE would enhance "interior" security while promoting information sharing with the FBI and developing stronger relationships with the U.S. Attorneys' Office.

An immigration enforcement agency with any role other than immigration enforcement was never formally considered by the Committee on the Judiciary or any other committee in Congress. As the legislative history surrounding passage of the Homeland Security Act underlines, and as the overwhelming passage of the Barbara Jordan Immigration Reform and Accountability Act further demonstrates, such dual or even multiple missions were expressly rejected by Congress.

PROVISIONS OF H.R. 1817 WITHIN THE JURISDICTION OF THE COMMITTEE ON THE JUDICIARY

There are several provisions contained in H.R. 1817 (as reported by the Committee on Homeland Security) that directly implicate the jurisdiction of the Committee. A summary of principal provisions follows.

Sec. 102. Border patrol agents

This section authorizes appropriations to hire an additional 2,000 border patrol agents. These 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. No. 108–458).

Sec. 107. State and local terrorism preparedness

This section authorizes appropriations for Fiscal Year 2006 for certain State and Local Terrorism Preparedness programs.

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

As reported from the Homeland Security Committee, this section authorizes $40 million (from the management and administration budget of the Bureau of Immigration and Customs Enforcement) to reimburse States along U.S. borders (30 miles or less from a border or coastline) for costs associated with having State and local law enforcement personnel trained and certified by the Immigration and Customs Enforcement (ICE) to enforce Federal immigration laws. The amendment strikes this section. The Homeland Security Committee lacks jurisdiction over this provision. In addition, if funding is authorized, all States (rather than those with borders or coastlines) should be reimbursed for costs associated with State and local law enforcement personnel training and certification by Federal immigration authorities.

Sec. 201. Terrorism Prevention Plan and related budget submission

This section authorizes the establishment of a Terrorist Prevention Plan (TPP) at DHS that encompasses: the identification and prioritization of the most significant threats presented by terrorist organizations; 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 counter-terrorism activities; specific initiatives by DHS to identify threats, coordinate activities within DHS to prevent acts of terrorism, and share information with state and local governments and the private sector. 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.

Sec. 202. Consolidated background check process

This section requires the Secretary of Homeland Security to create a single process for conducting security screening and background checks on individuals participating in voluntary or mandatory departmental credentialing or registered travel program.

Sec. 216. Authority for disseminating homeland security information

This section designates the Secretary of Homeland Security as the executive branch official responsible for the dissemination of homeland security information to State and local officials.

Sec. 222. Information collection requirements and priorities

This section amends section 102 of the Homeland Security Act of 2002 (Pub. L. No. 107–296) to add a provision that would make the Secretary of Homeland Security a member of any Federal interagency board that is responsible for establishing foreign collection

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. 301. National terrorism exercise program

This section establishes a National Terrorism Exercise Program for testing and evaluating the Nation's "capabilities to prevent * * * threatened or actual acts of terrorism * * * [and its] capability to detect, disrupt, and prevent threatened or actual catastrophic acts of terrorism."

Sec. 303. Review of antiterrorism acquisitions

This section requires the Secretary of DHS 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 (Pub. L. No. 107–296) (more commonly known as the "Support Anti-terrorism by Fostering Effective Technologies Act of 2002" or "SAFETY Act").

Sec. 311. Department of Homeland Security Cybersecurity Enhancement Act of 2005

This section establishes a cybersecurity office within the Department of Homeland Security, and requires the coordination of Federal, State and local officials to enhance cybersecurity cooperation.

Sec. 321. Security best practices

This section requires the submission of a report to Congress detailing best practices for enhancing the security of public transportation systems.

Sec. 332. Security review

This section requires the Secretary of Homeland Security, in coordination with "other relevant Federal agencies" to "review existing Federal, State, [and] local plans * * * for securing the critical infrastructure."

Sec. 401. Border security and enforcement coordination and operations

This section contains several findings concerning the implementation of the Homeland Security Act and the administration of Immigration and Customs Enforcement and border security missions. This section also contains broad conclusions concerning the division of resources within Immigration and Customs Enforcement and other immigration-related functions of the Department of Homeland Security, and makes specific recommendations concerning the proper organization of immigration-related functions at the Department of Homeland Security.

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. This section provides 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.

AMENDMENTS TO H.R. 1817 REPORTED BY THE COMMITTEE ON THE JUDICIARY

Sensenbrenner-Conyers Amendment to H.R. 1817

A bipartisan Manager's Amendment supported by Chairman Sensenbrenner and Ranking Member Conyers was reported from the Committee. This amendment made a number of changes to H.R. 1817 (as reported by the Committee on Homeland Security) that promote administrative efficiency and ensure against unnecessary duplication of responsibilities at DHS and other Federal agencies. A summary of this amendment and the changes made by the amendment are reflected below.

CRIMINAL LAW ENFORCEMENT PROVISIONS CONTAINED IN THE SENSENBRENNER-CONYERS AMENDMENT

Sec. 3. Definitions

Section 3 did not appear in H.R. 1817 as reported by the Homeland Security Committee. The phrases "prevent terrorist attacks" and "terrorism prevention" appear throughout the legislation. The term "terrorism prevention" can entail a number of different functions and responsibilities. Some of these functions are the responsibility of the DHS and some are the responsibility of other agencies such as the Department of Justice or the newly created Director of National Intelligence. In order to prevent unnecessary duplication, a definition of "terrorism prevention" was included in this section.

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

As reported from the Homeland Security Committee, this section authorizes $40 million (from the management and administration budget of the Bureau of Immigration and Customs Enforcement) to reimburse States along U.S. borders (30 miles or less from a border or coastline) for costs associated with having State and local law enforcement personnel trained and certified by the Immigration and Customs Enforcement (ICE) to enforce Federal immigration laws. The amendment strikes this section. The Homeland Security Committee lacks jurisdiction over this provision. In addition, if funding is authorized, the Committee believes all States (rather than those with borders or coastlines) should be reimbursed for

costs associated with State and local law enforcement personnel training and certification by Federal immigration authorities.

Sec. 201. Terrorism prevention plan and related budget submission

As reported by the Committee on Homeland Security, this section authorizes DHS to expand its powers beyond the statutory authority. The Sensenbrenner-Conyers amendment reported by the Committee clarifies the authority of DHS in relation to law enforcement and intelligence agencies in order to better reflect the mission of the DHS and to promote administrative efficiency within DHS and other Federal agencies. Specifically, the amendment clarifies DHS authority to identify vulnerabilities of the United States to terrorist attacks and use this information to prevent terrorist attacks by securing our borders, securing critical infrastructure, disseminating homeland security information to Federal, State and local governments, and preparing first responders for terrorist attacks. The changes to this section are essential to clarify the proper role of the DHS and avoid duplication and turf battles among competing Federal agencies in the fight against terrorism. Each agency has a role in this fight which has been established by Congress, and the responsibilities should be reinforced by this legislation. The legislation, as amended by the Committee on Homeland Security, would create confusion about the roles and responsibilities of the Federal agencies.

Sec. 202. Consolidated background check process

The Sensenbrenner-Conyers amendment to this section preserves DHS authority to administer a consolidated background check process but inserts "in consultation with the Attorney General." The Attorney General requires consultation because criminal background checks often involve the resources of the Department of Justice.

Sec. 216. Authority for Disseminating Homeland Security Information

As reported by the Committee on Homeland Security, this section provides DHS with sole authority to disseminate "homeland security" information to State and local government agencies and would prohibit other agencies from sharing such information. An exception would be made for information necessary for criminal justice purposes. It is unclear what the terms "homeland security information" and "criminal justice purposes" entail. The amendment would establish the Department of Homeland Security as the principal agency for the dissemination of homeland security information, but eliminates the prohibition on other Federal agencies as well as the exception.

Sec. 218. Access to nuclear terrorism-related information

As reported by the Homeland Security Committee, this section requires any component of DHS that receives information related to a nuclear threat to disseminate that information throughout the Department and to State and local governments. The Sensenbrenner-Conyers amendment expands the list of recipients of information pertaining to nuclear threats to include other Federal agencies.

Sec. 222. Information collection requirements and priorities

As reported, this section required the President to include the Secretary of DHS on any interagency board responsible for collection of foreign intelligence information. The amendment eliminates this requirement and retains executive discretion for such appointments. As reported, this section would have also established an interagency board, chaired by the Secretary of DHS, which also included the Attorney General and the Director of National Intelligence among others, to coordinate the collection of information related to homeland security and prioritize the collection and use of such information. The Sensenbrenner-Conyers amendment eliminates this provision because these duties are properly performed by the newly created Director of National Intelligence and respective Federal agencies.

Sec. 301. National terrorism exercise program

This section authorizes the Secretary of Homeland Security to conduct the TOPOFF (simulated terrorism attack exercise) program to train State and local first responders in responding and preventing terrorist attacks. Because DHS exercises would involve the active participation of Federal law enforcement agencies, the Sensenbrenner-Conyers amendment would require the Secretary of DHS to coordinate with the Attorney General and the Director of National Intelligence when developing such exercises.

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

This section requires the Secretary of Homeland Security to provide a report to the Committee on Homeland Security regarding terrorist threats to agriculture. The Sensenbrenner-Conyers amendment would require the report to be additionally submitted to the Committee on the Judiciary.

Sec. 331. Critical infrastructure

This section requires the Secretary of Homeland Security to prioritize threats to the Nation's critical infrastructure. The Sensenbrenner-Conyers amendment would require the Secretary to consult with the Attorney General and the Director of National Intelligence in developing this analysis.

Sec. 333. Implementation report

This section requires the Secretary to submit a report to the Committee on Homeland Security regarding plans for securing the critical infrastructure. The Sensenbrenner-Conyers amendment requires the report to be submitted to the Committee on Judiciary as well.

Sec. 405. Denial of transportation security card

This section was added to the bill by the Transportation Committee. It would prohibit the Secretary from using a felony conviction that is more than seven years old and not terrorism related to make a determination that an applicant poses a terrorism security risk for purposes of denying a person a Transportation Security Card. Such a card may be used to gain access to hazmat credentials, ports, and railroads. The Sensenbrenner-Conyers reported

by the Committee modifies this section to prohibit the Secretary from using a non-terrorism related felony conviction as the sole reason for determining that an applicant poses a terrorism security risk for purposes of denying a person a Transportation Security Card.

IMMIGRATION-RELATED PROVISIONS CONTAINED IN THE SENSENBRENNER-CONYERS AMENDMENT

Sec. 102. Border patrol agents

This section authorizes appropriations to hire an additional 2,000 border patrol agents. These 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 (Pub. L. No. 108–458). The Sensenbrenner-Conyers amendment authorizes the appropriation of sufficient funds for the Immigration and Customs Enforcement (ICE) Legal Program for the hiring of an additional 300 attorneys and related training and support costs, and authorizes such sums as may be necessary for Citizenship and Immigration Services (CIS) to hire an additional 300 adjudicators and related training and support costs to carry out the adjudicative functions specified in section 451(b) of the Homeland Security Act of 2002.

The legacy INS General Counsel program consisted of 710 attorneys. Most of these attorneys were assigned to Immigration Court. The newly formed ICE lost 135 positions to the Bureau of Customs and Border Protection (CBP) and CIS. However, no attorneys at either of those two agencies represent the United States in removal proceedings. As a result, to properly staff all removal proceedings and handle other responsibilities, the ICE Principal Legal Advisor's Office has 587 attorneys. INS attorneys as a whole faced an increasing workload even before the creation of DHS, a problem that has been exacerbated by ICE's loss of attorneys. In 2004, ICE attorneys had time to spend only 23 minutes preparing the average case for hearing. The U.S. Army Manpower Analysis Agency had completed a review of the INS legal program's staffing needs in 1998 and found that "the Legal Proceedings Program is vastly understaffed and underfunded. Its attorneys cannot adequately perform their assigned functions without significant increases in personnel. Based on its FY 1997 workload, the program needs * * * an additional * * * 293 attorneys * * *." The role that a lack of attorney resources played in terrorist planning is evident from the 9/11 Terrorist Travel Monograph, which describes how terrorists exploited U.S. immigration laws before the 2001 attacks: "Aliens were granted multiple hearings, often resulting in lengthy delays. This system was easy to exploit. Because the immigration attorneys representing the INS in cases against aliens worked solely from paper files, they were often unable to properly track cases or access the necessary files to present their cases efficiently and knowledgeably. For much of the 1990s, case backlogs were considerable. Terrorists knew they could beat the system—and, as we have seen, they often did."

CIS faces a backlog of approximately 1.3 million applications (that number doubles if one includes the cases pending without a

current available visa number). There was a recent hiring freeze at CIS, and in addition there has been a "backlog" in hiring because new CIS employees must undergo a time consuming security clearance by the Office of Personnel Management because CIS's private sector recruiter went out of business. Most employees at CIS are currently working many hours of overtime to help reduce the backlog. Of course, legislative proposals to increase premium processing and institute a large-scale guest worker program would require many more adjudicators. Recent briefings by the Government Accountability Office reveal that CIS has determined that channeling funding towards electronic filing would be less advantageous than hiring more adjudicators and would only delay backlog reduction efforts.

Sec. 401. Border security and enforcement coordination and operations

As reported by the Committee on Homeland Security, Section 401 contains a number of findings regarding the creation and function of the Bureau of Border Security pursuant to the Homeland Security Act of 2002 and the advisability of the Administration's creation of ICE and CBP when establishing the Department of Homeland Security. The section also provides that the Secretary of Homeland Security shall evaluate the organizational structure of DHS, especially as it relates to ICE and CBP. The Sensenbrenner-Conyers amendment ensures that the Secretary of Homeland Security will study the rationale and consequences of both of these organizational decisions of the Administration, and not just the decision to bifurcate immigration enforcement. The amendment also ensures that the findings of section 401 as reported by the Committee on Homeland Security do not prejudge the issues.

ADDITIONAL AMENDMENTS TO H.R. 1817 ADOPTED BY THE COMMITTEE ON THE JUDICIARY

In addition to the Sensenbrenner-Conyers amendment, the Committee on the Judiciary reported three amendments to H.R. 1817 by voice vote.

The Committee adopted an amendment offered by Mr. Delahunt that authorizes sufficient funding for the development of a regional homeland security center that enhances coordination for terrorism preparedness among all levels of government. The Federal government can realize significant financial savings by maximizing regional infrastructure and capabilities in high-risk regions throughout the United States. To ensure efficient allocation of resources, the amendment specifies that any authorization of funding will be contingent upon the completion of a feasibility study, conducted by the Federal government, to determine the most appropriate location for its establishment. Last year, the Department of Defense completed an extensive and comprehensive feasibility study that concluded that a regional Homeland Defense Training Center is needed for the New England region.

The Committee adopted an amendment offered by Mr. Weiner that authorizes Homeland Security grant funding for the salaries of "Terrorism Cops" hired exclusively for terrorism or homeland security purposes.

The Committee adopted an amendment offered by Ms. Jackson-Lee that requires the Secretary of Homeland Security to collect data on the use of "immigration consultants" by aliens if the alien states that he or she used the service of an immigration consultant or a Department employee suspects that the alien used the services of an immigration consultant. There are a rising number of consultants that illegally practice immigration law without a license.

HEARINGS

H.R. 1817 was introduced on April 26, 2005. No hearings were held on the legislation. However, since the establishment of the Department of Homeland Security, the Committee on the Judiciary held several hearings examining the operation of components of the Department within the Committee's jurisdiction.

HEARINGS BEFORE THE SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

On June 4, 2002, the Subcommittee on Crime, Terrorism, and Homeland Security conducted a legislative hearing on H.R. 4598, the "Homeland Security Information Sharing Act," at which the following witnesses testified: Senator Saxby Chambliss (R-GA); Rep. Jane Harman (D-CA); John Bittick, President of the National Sheriffs' Association.

On June 9, 2002, the Subcommittee on Crime, Terrorism, and Homeland Security conducted an oversight hearing on the "Proposal to Create a Department of Homeland Security," at which the following witnesses testified: Rep. Lamar Smith (R–TX); Robert Bonner, Commission of the U.S. Customs Service; Thomas Collins, Commandment of the United States Coast Guard; John Magaw, Under Secretary of Transportation and Security at the Transportation Security Administration; Brian L. Stafford, Director of the United States Secret Service.

On June 25, 2002, the Subcommittee on Crime, Terrorism, and Homeland Security conducted an oversight hearing on the "Risk to Homeland Security From Identity Fraud and Identity Theft," at which the following witnesses testified: Paul McNulty, United States Attorney; James G. Huse, Inspector General at the Social Security Administration; Richard M. Stana, Director of Administration of Justice Issues, U.S. General Accounting Office; Edmund Mierzwinski, Consumer Program Director for the State Public Interest Research Groups.

On November 20, 2003 the Subcommittee on Crime, Terrorism, and Homeland Security conducted a legislative/oversight hearing on "Homeland Security—the Balance Between Crisis and Consequence Management Through Training and Assistance (Review of Legislative Proposals H.R. 2512, H.R. 3266 and H.R. 3158)," at which the following witnesses testified: William Bishop, Director of Homeland Security in the State of Idaho; Raymond W. Kelly, Police Commissioner for the City of New York; Susan Mencer, Director of the Office of Domestic Preparedness at the Department of Homeland Security.

On February 3, 2004 the Subcommittee on Crime, Terrorism, and Homeland Security conducted an oversight hearing on the "Law Enforcement Efforts Within the Department of Homeland Secu-

rity," at which the following witnesses testified: W. Ralph Basham, Director of the United States Secret Service at the Department of Homeland Security; Thomas Collins, Commandant of the United States Coast Guard at the Department of Homeland Security; Michael Garcia, Assistant Secretary for the Bureau of Immigration and Customs Enforcement at the Department of Homeland Security.

HEARINGS BEFORE THE SUBCOMMITTEE ON IMMIGRATION, BORDER SECURITY, AND CLAIMS

On April 10, 2003, the Subcommittee on Immigration, Border Security, and Claims held an oversight hearing on "Department of Homeland Security Transition: Bureau of Immigration and Customs Enforcement," at which the following witnesses testified: Under Secretary Asa Hutchinson, Border and Transportation Security, Department of Homeland Security; Mark Krikorian, Executive Director, Center for Immigration Studies; Timothy Danahey, Federal Law Enforcement Officers Association (FLEOA); and Rich Stana, Director for Homeland Security and Justice Issues, General Accounting Office.

On May 8, 2003, the Subcommittee on Immigration, Border Security, and Claims held an oversight hearing on "War on Terrorism: Immigration Enforcement Since September 11, 2001," at which the following witnesses testified: Kevin Rooney, Director, Executive Office for Immigration Review, Department of Justice; Michael Dougherty, Director of Operations, Bureau of Immigration and Customs Enforcement, Department of Homeland Security; Jay Ahern, Assistant Commissioner, Office of Field Operations, Bureau of Customs and Border Protection, Department of Homeland Security; and Laura Murphy, American Civil Liberties Union.

On February 25, 2004, the Subcommittee on Immigration, Border Security, and Claims held an oversight hearing on "Funding for Immigration in the President's 2005 Budget," at which the following witnesses testified: Eduardo Aguirre, Director, Citizenship and Immigration Services; Michael Dougherty, Director of Operations, Immigration and Customs Enforcement; Daniel Smith, Principal Deputy Assistant Secretary for Consular Affairs, Department of State; and Seth Stodder, Counselor and Senior Policy Advisor to Commissioner Robert C. Bonner, U.S. Customs and Border Protection.

On March 4, 2004, the Subcommittee on Immigration, Border Security, and Claims held an oversight hearing on "Alien Removal Under Operation Predator," at which the following witnesses testified: Michael J. Garcia, Assistant Secretary for U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security; and John Walsh, Host of "America's Most Wanted: America Fights Back."

On March 11, 2004, the Subcommittee on Immigration, Border Security, and Claims held an oversight hearing on "Funding for Immigration in the President's 2005 Budget," at which the following witnesses testified: T.J Bonner, President, National Border Patrol Council; Timothy J. Danahey, National President, Federal Law Enforcement Officers Association (FLEOA); and Demetrios Papademetriou, Senior Associate & Co-Director, Migration Policy Institute (MPI).

On March 18, 2004, the Subcommittee on Immigration, Border Security, and Claims held an oversight hearing on "US VISIT–A Down Payment on Homeland Security," at which the following witnesses testified: Mr. Robert M. Jacksta, Executive Director, Border Security and Facilitation, U.S. Customs and Border Protection, U.S. Department of Homeland Security; Mr. Robert A. Mocny, Deputy Director, US–VISIT Office, Department of Homeland Security; Mr. Alfonso Martinez-Fonts, Jr., Special Assistant to the Secretary for the Private Sector, U.S. Department of Homeland Security; and Mr. Randolph C. Hite, Director, Information Technology Architecture and Systems Issues, U.S. General Accounting Office.

On June 17, 2004, the Subcommittee on Immigration, Border Security, and Claims conducted an oversight hearing on "Families and Businesses in Limbo: The Detrimental Impact of the Immigration Backlog," at which the following witness testified: The Honorable Eduardo Aguirre, Director of U.S. Citizenship and Immigration Services, U.S. Department of Homeland Security.

On June 23, 2004, the Subcommittee on Immigration, Border Security, and Claims conducted an oversight hearing on "Families and Businesses in Limbo: The Detrimental Impact of the Immigration Backlog," at which the following witnesses testified: Mr. Prakash Khatri, Citizenship and Immigration Services Ombudsman, U.S. Department of Homeland Security; Ms. Elizabeth Stern, Managing Partner, Business Immigration Practice Group, Shaw Pittman, LLC; and Mr. Paul Zulkie, President, American Immigration Lawyers Association.

On March 3, 2005, the Subcommittee on Immigration, Border Security, and Claims conducted an oversight hearing on "The Immigration Enforcement Resources Authorized in the Intelligence Reform and Terrorism Prevention Act of 2004," at which the following witnesses testified: Rep. Solomon P. Ortiz, 27th District of Texas; Mr. Peter Gadiel, 9–11 Families for a Secure America; Mr. T.J. Bonner, President, National Border Patrol Council; and Mr. Robert Eggle, Father of Kris Eggle, slain National Park Service Ranger.

On March 10, 2005, the Subcommittee on Immigration, Border Security, and Claims conducted an oversight hearing on "Interior Immigration Enforcement Resources," at which the following witnesses testified: Mr. Paul Martin, Deputy Inspector General, U.S. Department of Justice; Mr. Michael Cutler, Former I.N.S. Special Agent; Mr. Randy Callahan, Vice President, National Homeland Security Council; and Dr. Craig Haney, Professor, University of California at Santa Cruz.

On May 5, 2005, the Subcommittee on Immigration, Border Security, and Claims conducted an oversight hearing on the "New 'Dual Missions' of the Immigration Enforcement Agencies," at which the following witnesses testified: Michael Cutler, former INS Special Agent; T.J. Bonner, President of the National Border Patrol Council; Janice Kephart, Former September 11 Commission Staff Counsel; and Richard Stana, Director of Homeland Security and Justice Issues at the U.S. Government Accountability Office.

HEARINGS BEFORE THE SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

On February 10, 2004 the Subcommittee on Commercial and Administrative Law conducted an oversight hearing on "Privacy in

the Hands of the Government: The Privacy Officer for the Department of Homeland Security," at which the following witnesses testified: James Dempsey, Executive Director for the Center for Democracy and Technology; James S. Gilmore III, President of the USA Secure Corporation; Sally Katzen, visiting professor at the University of Michigan School of Law; Nuala O'Connor Kelly, Chief Privacy Officer at the Department of Homeland Security.

COMMITTEE CONSIDERATION

On May 12, 2005, the Committee met in open session and ordered favorably reported the bill H.R. 1817, as amended, by a voice vote, a quorum being present.

VOTE OF THE COMMITTEE

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee notes that [there were no recorded votes during the committee consideration of H.R. 1817 the following roll call votes occurred during the committee's consideration of H.R. 1817.

1. Mr. Hostettler offered an amendment that would have created whistleblower protections and monetary rewards for persons who contribute to successful prosecutions of employers unlawfully employing aliens. The amendment was defeated by a vote of 12 ayes and 16 nays.

Member	Ayes	Nays	Present
Mr. Hyde			
Mr. Coble	X		
Mr. Smith	X		
Mr. Gallegly	X		
Mr. Goodlatte			
Mr. Chabot			
Mr. Lungren		X	
Mr. Jenkins	X		
Mr. Cannon		X	
Mr. Bachus			
Mr. Inglis	X		
Mr. Hostettler	X		
Mr. Green		X	
Mr. Keller		X	
Mr. Issa		X	
Mr. Flake			
Mr. Pence	X		
Mr. Forbes	X		
Mr. King	X		
Mr. Feeney	X		
Mr. Franks			
Mr. Gohmert			Pass
Mr. Conyers	X		
Mr. Berman			
Mr. Boucher			
Mr. Nadler		X	
Mr. Scott		X	
Mr. Watt		X	
Ms. Lofgren			
Ms. Jackson Lee		X	
Ms. Waters	X		
Mr. Meehan		X	
Mr. Delahunt		X	
Mr. Wexler			
Mr. Weiner		X	

Member	Ayes	Nays	Present
Mr. Schiff		X	
Ms. Sanchez		X	
Mr. Smith			
Mr. Van Hollen		X	
Mr. Sensenbrenner, Chairman		X	
Total	12	16	1

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee reports that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 3(c)(2) of rule XIII of the Rules of the House of Representatives is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 1817, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

MAY 13, 2005.

Hon. F. JAMES SENSENBRENNER, Jr.,
Chairman, Committee on the Judiciary,
U.S. House of Representatives, Washington DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 1817, the Department of Homeland Security Authorization Act for Fiscal Year 2006.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Mark Grabowicz (for federal costs) and Melissa Merrell (for the impact on state and local governments).

Sincerely,

DOUGLAS HOLTZ-EAKIN,
Director.

Enclosure.

H.R. 1817—Department of Homeland Security Authorization Act for Fiscal Year 2006

Summary: H.R. 1817 would authorize the appropriation of $34.2 billion for fiscal year 2006 to fund the major operations of the Department of Homeland Security (DHS). CBO estimates that implementing H.R. 1817 would cost about $33 billion over the 2006–2010 period, assuming appropriation of the authorized amounts. Enacting the bill would not affect direct spending or receipts.

H.R. 1817 contains an intergovernmental mandate as defined in the Unfunded Mandates Reform Act (UMRA) by exempting certain information related to critical infrastructure from state and local laws that provide public access to information. CBO estimates that the costs, if any, to state and local governments would be minimal and well below the annual threshold established in that act ($62 million in 2005, adjusted annually for inflation). H.R. 1817 contains no new private-sector mandates as defined in UMRA.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 1817 is shown in the following table. For this estimate, CBO assumes that the authorized amounts will be appropriated near the beginning of fiscal year 2006 and that outlays will follow the historical spending rates for these activities. The costs of this legislation fall within budget functions 050 (national defense), 300 (natural resources and environment), 400 (transportation), 450 (community and regional development), 550 (health), 600 (income security), 750 (administration of justice), and 800 (general government).

	By fiscal year, in millions of dollars—					
	2005	2006	2007	2008	2009	2010
SPENDING SUBJECT TO APPROPRIATION						
Department of Homeland Security:						
Spending Under Current Law:						
Estimated Budget Authority [a]	38,469	0	0	0	0	0
Estimated Outlays	31,928	14,443	7,939	3,475	1,308	594
Proposed Changes:						
Authorization Level	0	34,152	0	0	0	0
Estimated Outlays	0	17,418	7,513	5,123	2,391	683
Department of Homeland Security:						
Spending Under H.R. 1817:						
Authorization Level [a]	38,469	34,152	0	0	0	0
Estimated Outlays	31,928	31,861	15,452	8,598	3,699	1,277

[a] The estimated 2005 level is the amount of appropriations less offsetting collections for that year for operations of DHS.

Intergovernmental and private-sector impact: H.R. 1817 contains an intergovernmental mandate as defined in UMRA by exempting certain information related to critical infrastructure from state and local laws that provide public access to information. CBO estimates that the costs, if any, to state and local governments would be minimal and well below the annual threshold established in that act ($62 million in 2005, adjusted annually for inflation). H.R. 1817 contains no new private-sector mandates as defined in UMRA.

Section 306 would require the Secretary of the Department of Homeland Security to issue regulations for the security of maritime cargo moving within the intermodal transportation system. Those regulations would relate to the securing, recording, and verifying of seals on maritime cargo containers in the hauling of cargo from one mode of transportation to another. According to DHS, a notice of proposed rulemaking that incorporates the recommendations referred to in the bill has been drafted and is pending review. Based on information from DHS, CBO anticipates that the Secretary will issue those regulations. Thus, CBO expects that the provisions in this section would impose no additional mandates on public or private-sector entities.

State and local governments would benefit from programs to improve interoperable communications and training and from changes

to existing grants that allow funds to be used to pay for the salaries of certain law enforcement officers. Any costs incurred by those governments would be incurred voluntarily.

Previous CBO estimates: On May 6, 2005, CBO transmitted a cost estimate for H.R. 1817 as ordered reported by the House Committee on Homeland Security on April 27, 2005. On May 13, 2005, CBO transmitted a cost estimate for H.R. 1817 as ordered reported by the House Committee on Energy and Commerce on May 11, 2005. The three versions of the bill are similar, and all three cost estimates are identical.

Estimate prepared by: Federal costs: Mark Grabowicz; impact on state, local, and tribal governments: Melissa Merrell; impact on the private sector: Paige Piper/Bach.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

PERFORMANCE GOALS AND OBJECTIVES

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 1817 would authorize the Department of Homeland Security for Fiscal Year 2006.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds the authority for this legislation in article I, section 8 of the Constitution.

SECTION-BY-SECTION ANALYSIS AND DISCUSSION

The following is a discussion of sections within the jurisdiction of the Committee on the Judiciary. The other sections are described in the report to accompany this legislation prepared by the Committee on Homeland Security (H.R. Rep. No. 109–71 Part I).

Sec. 3. Definitions

Section 3 did not appear in H.R. 1817 as reported by the Homeland Security Committee. In order to prevent unnecessary duplication, a definition of "terrorism prevention" was included in this section.

Sec. 102. Border Patrol agents

This section authorizes appropriations to hire an additional 2,000 Border Patrol agents. These 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. No. 108–458). As amended by the Committee on the Judiciary, this section authorizes the appropriation of sufficient funds for the Immigration and Customs Enforcement (ICE) Legal Program for the hiring of an additional 300 attorneys and related training and support costs, and authorizes such sums as may be necessary for Citizenship and Immigration Services (CIS) to hire an additional 300 adjudicators and related training and support costs to carry out the adjudicative functions specified in section 451(b) of the Homeland Security Act of 2002.

Sec. 107. State and local terrorism preparedness

This section authorizes appropriations for Fiscal Year 2006 for certain State and Local Terrorism Preparedness programs. The Committee adopted an amendment offered by Mr. Weiner that authorizes Homeland Security grant funding for the salaries of "Terrorism Cops" hired exclusively for terrorism or homeland security purposes. In addition, the Committee adopted an amendment offered by Mr. Delahunt that authorizes sufficient funding for the development of a regional homeland security center that enhances coordination for terrorism preparedness among all levels of government. The Federal government can realize significant financial savings by maximizing regional infrastructure and capabilities in high-risk regions throughout the United States. To ensure efficient allocation of resources, the amendment specifies that any authorization of funding will be contingent upon the completion of a feasibility study, conducted by the Federal government, to determine the most appropriate location for its establishment.

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

As reported from the Homeland Security Committee, this section authorizes $40 million (from the management and administration budget of the Bureau of Immigration and Customs Enforcement) to reimburse States along U.S. borders (30 miles or less from a border or coastline) for costs associated with having State and local law enforcement personnel trained and certified by the Immigration and Customs Enforcement (ICE) to enforce Federal immigration laws. The Committee reported an amendment to strike this section. The Homeland Security Committee lacks jurisdiction over this provision. In addition, if funding is authorized, all States (rather than those with borders or coastlines) should be reimbursed for costs associated with State and local law enforcement personnel training and certification by Federal immigration authorities.

Sec. 201. Terrorism prevention plan and related budget submission

As reported by the Committee on Homeland Security, this section authorizes DHS to expand its powers beyond the authority granted to that agency in its original authorizing legislation. The amendment clarifies the authority of DHS in relation to law enforcement and intelligence agencies in order to better reflect the mission of the DHS and to promote administrative efficiency within DHS and other federal agencies.

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. This section authorizes the creation of a consolidated background check process. The amendment to this section reported by the Committee preserves DHS authority to administer a consolidated background check process but inserts "in consultation with the Attorney General." The Attorney General requires consultation because criminal background checks often involve the resources of the Department of Justice.

Sec. 216. Authority for disseminating homeland security information

As reported by the Committee on Homeland Security, this section provides DHS with sole authority to disseminate "homeland security" information to State and local government agencies and would prohibit other agencies from sharing such information. An exception would be made for information necessary for criminal justice purposes. It is unclear what the terms "homeland security information" and "criminal justice purposes" entail. As amended by the Committee on the Judiciary, the amendment recognizes DHS as the principal agency for the dissemination of homeland security information, but eliminates the prohibition on other Federal agencies as well as the exception.

Sec. 218. Access to nuclear terrorism-related information

This section requires any component of DHS that receives information related to a nuclear threat to disseminate that information throughout the Department and to State and local governments. The Sensenbrenner-Conyers amendment expands the list of recipients of information pertaining to nuclear threats to include other Federal agencies.

Sec. 222. Information collection requirements and priorities

As reported, this section required the President to include the Secretary of DHS on any interagency board responsible for collection of foreign intelligence information. The amendment eliminates this requirement and retains executive discretion for such appointments. As reported, this section would have also established an interagency board, chaired by the Secretary of DHS, which also included the Attorney General and the Director of National Intelligence among others, to coordinate the collection of information related to homeland security and prioritize the collection and use of such information. The Sensenbrenner-Conyers amendment reported by the Committee eliminates this provision because these duties are properly performed by the newly created Director of National Intelligence and respective Federal agencies.

Sec. 301. National terrorism exercise program

This section authorizes the Secretary of Homeland Security to conduct the TOPOFF (simulated terrorism attack exercise) program to train State and local first responders in responding and preventing terrorist attacks. Because DHS exercises would involve the active participation of Federal law enforcement agencies, the Sensenbrenner-Conyers amendment modifies this section to require the Secretary of DHS to coordinate with the Attorney General and the Director of National Intelligence when developing such exercises.

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

This section requires the Secretary of Homeland Security to provide a report to the Committee on Homeland Security regarding terrorist threats to agriculture. As amended by the Committee, this section would require the report be additionally submitted to the Judiciary Committee.

Sec. 331. Critical infrastructure

This section requires the Secretary of Homeland Security to prioritize threats to the Nation's critical infrastructure. The amendment reported from the Judiciary Committee requires the Secretary to consult with the Attorney General and the Director of National Intelligence in developing this analysis.

Sec. 333. Implementation report

This section requires the Secretary to submit a report to the Committee on Homeland Security regarding plans for securing the critical infrastructure. This section was amended by the Committee to the report to be submitted to the Committee on the Judiciary as well.

Sec. 405. Denial of transportation security card

This section was added to the bill by the Transportation Committee. It would prohibit the Secretary from using a felony conviction that is more than seven years old and not terrorism related to make a determination that an applicant poses a terrorism security risk for purposes of denying a person a Transportation Security Card. Such a card may be used to gain access to hazmat credentials, ports, and railroads. This section was amended by the Committee to prohibit the Secretary from using a non-terrorism related felony conviction as the sole reason for determining that an applicant poses a terrorism security risk for purposes of denying a person a Transportation Security Card.

Sec. 407. Data collection on use of immigration consultants

Section 407 did not appear in H.R. 1817 as reported by the Committee on Homeland Security. Offered by Ms. Jackson-Lee, this new section requires the Secretary of Homeland Security to collect data on the use of "immigration consultants" by aliens if the alien states that he or she used the service of an immigration consultant or a Department employee suspects that the alien used the services of an immigration consultant. There are a rising number of consultants that illegally practice immigration law without a license.

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. 104. AUTHORITY FOR DISSEMINATING HOMELAND SECURITY INFORMATION.

The Secretary shall be the principal executive branch official responsible for disseminating homeland security information to State and local government and tribal officials and the private sector.

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 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.

(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 Federal, 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 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.

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 infra-

structure 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, in concurrence with the Attorney General and the National Director of Intelligence, 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;

(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 se-

curity card that includes notice and an opportunity for a hearing *before an administrative law judge*.

* * * * * * *

(5) In making a determination under paragraph (1)(D) that an individual poses a terrorism security risk, the Secretary shall not consider, as the sole reason, 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 an offense that is a violation of a provision specified in subparagraph (B) of section 2332b(g)(5) of title 18.

* * * * * * *

○