109TH CONGRESS 2d Session } HOUSE OF REPRESENTATIVES { REPT. 109–729 Part 1

HOMELAND SECURITY SCIENCE AND TECHNOLOGY ENHANCEMENT ACT OF 2006

DECEMBER 8, 2006.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

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

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 4941]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 4941) to reform the science and technology programs and activities of the Department of Homeland Security, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
Amendment	2
Purpose and Summary	11
Background and Need for Legislation	11
Hearings	12
Committee Consideration	12
Committee Votes	12
Committee Oversight Findings	21
Statement of General Performance Goals and Objectives	21
New Budget Authority, Entitlement Authority, and Tax Expenditures	21
Congressional Budget Office Estimate	22
Federal Mandates Statement	23
Compliance With House Resolution 1000	23
Advisory Committee Statement	23
Constitutional Authority Statement	24
Applicability to Legislative Branch	24
Section-by-Section Analysis of the Legislation	24

59–006

Changes in Existing Law Made by the Bill, as Reported 33
Additional Views 43

AMENDMENT

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 "Homeland Security Science and Technology Enhancement Act of 2006".

SEC. 2. NATIONAL STANDARDS FOR HOMELAND SECURITY EQUIPMENT AND TRAINING.

(a) AMENDMENT.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.) is amended by adding at the end the following new section:

"SEC. 314. NATIONAL STANDARDS FOR HOMELAND SECURITY EQUIPMENT AND TRAINING.

"(a) EQUIPMENT STANDARDS.—

"(1) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, and in consultation with other components of the Department, as appropriate, and the National Institute of Standards and Technology, shall support the development, promulgation, and updating as necessary of national voluntary consensus standards for the performance, use, and validation of equipment used by Federal, State, and local government and nongovernment emergency response providers, and by the components of the Department. Such standards—

"(A) shall be, to the maximum extent practicable, consistent with any existing voluntary consensus standards;

"(B) shall take into account, as appropriate, new types of terrorism threats and responsibilities of the Department that may not have been contemplated when such existing standards were developed;

"(C) shall be focused on maximizing interoperability, interchangeability, durability, flexibility, efficiency, efficacy, portability, sustainability, and safety; and

"(D) shall cover all appropriate uses of the equipment.

"(2) REQUIRED CATEGORIES.—In carrying out paragraph (1), the Secretary shall specifically consider national voluntary consensus standards for the performance, use, and validation of the following categories of equipment:

"(A) Thermal imaging equipment.

"(B) Radiation detection and analysis equipment.

"(C) Biological detection and analysis equipment.

"(D) Chemical detection and analysis equipment.

"(E) Decontamination and sterilization equipment.

"(F) Personal protective equipment, including garments, boots, gloves, and hoods and other protective clothing.

"(G) Respiratory protection equipment.

"(H) Interoperable communications, including wireless and wireline voice, video, and data networks.

"(I) Explosive detection and analysis equipment, and technologies and methods to mitigate the impact of explosive devices or materials.

"(J) Containment vessels.

"(K) Contaminant-resistant vehicles.

"(L) Aerial platforms.

"(M) Special rescue equipment.

"(N) Screening and patrolling technologies.

"(O) Such other equipment for which the Secretary determines that national voluntary consensus standards would be appropriate.

"(3) CERTIFICATION AND ACCREDITATION.—The Secretary, in carrying out this subsection, and in coordination with the Director of the National Institute of Standards and Technology, may support the certification of equipment and the accreditation of laboratories to conduct testing and evaluation.

"(4) EQUIPMENT STANDARDS AND ACQUISITIONS.—

"(A) DEPARTMENT SUPPORTED ACQUISITIONS.—If an applicant for financial assistance provided by the Department proposes to use such financial assistance to upgrade or purchase new equipment or systems that do not meet or exceed any applicable national voluntary consensus standards, the applicant shall include in its application for financial assistance an explanation of why such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed such standards.

"(B) DEPARTMENT ACQUISITIONS.—When an operational unit of the Department proposes to upgrade or purchase new equipment or systems, the head of that unit shall consult with the Under Secretary for Science and Technology on whether such equipment or systems meet or exceed any applicable national voluntary consensus standards and whether there is need for the Department to support the development or updating of applicable national voluntary consensus standards.

"(b) TRAINING STANDARDS.—

"(1) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, and in consultation with other components of the Department, as appropriate, shall support the development, promulgation, and regular updating as necessary of national voluntary consensus standards for training for Federal, State, and local government and nongovernment emergency response providers and Department personnel, including training that will enable them to use equipment effectively and appropriately in carrying out their responsibilities. Such standards shall give priority to providing training to—

"(A) enable Federal, State, and local government and nongovernment emergency response providers and Department personnel to prevent, prepare for, respond to, mitigate against, and recover from terrorist threats, including threats from chemical, biological, radiological, and nuclear weapons and explosive devices capable of inflicting significant human casualties, and other emergencies; and

"(B) familiarize Federal, State, and local government and nongovernment emergency response providers and Department personnel with the proper use of equipment, including software, developed pursuant to the standards developed under subsection (a).

"(2) REQUIRED CATEGORIES.—In carrying out paragraph (1), the Secretary specifically shall include the following categories of activities:

"(A) Regional planning.

"(B) Joint exercises.

"(C) Intelligence collection, analysis, and sharing.

"(D) Decisionmaking protocols for incident response and alarms.

"(E) Emergency notification of affected populations.

"(F) Detection of biological, nuclear, radiological, and chemical weapons of mass destruction.

"(G) Screening and patrolling procedures.

"(H) Such other activities for which the Secretary determines that national voluntary consensus training standards would be appropriate.

"(3) CONSISTENCY.—In carrying out this subsection, the Secretary shall ensure that—

"(A) training standards for Federal, State, and local government and nongovernment emergency response providers are consistent with the principles of emergency preparedness for all hazards; and

"(B) training standards for Department personnel are consistent with the counterterrorism and traditional responsibilities of the Department.

"(c) CONSULTATION WITH STANDARDS ORGANIZATIONS.—In supporting the development, promulgation, and updating of national voluntary consensus standards for equipment for and training under this section, the Secretary shall consult with relevant public and private sector groups, including—

"(1) the National Institute of Standards and Technology;

"(2) the National Fire Protection Association;

"(3) the National Association of County and City Health Officials;

"(4) the Association of State and Territorial Health Officials;

"(5) the American National Standards Institute;

"(6) the National Institute of Justice;

"(7) the Inter-Agency Board for Equipment Standardization and Interoperability;

"(8) the National Public Health Performance Standards Program;

"(9) the National Institute for Occupational Safety and Health;

"(10) ASTM International;

"(11) the International Safety Equipment Association;

"(12) the Emergency Management Accreditation Program; and

"(13) to the extent the Secretary considers appropriate, other national voluntary consensus standards development organizations, other interested Federal, State, and local agencies, and other interested persons.

"(d) COORDINATION WITH SECRETARIES OF HHS AND TRANSPORTATION.—In supporting the development, promulgation, and updating of any national voluntary consensus standards under this section for equipment for or training of emergency re-

sponse providers that involve or relate to health or emergency medical services professionals, including emergency medical professionals, the Secretary shall coordinate activities under this section with the Secretary of Health and Human Services and the Secretary of Transportation.

"(e) CONSISTENCY WITH THE NATIONAL TECHNOLOGY TRANSFER AND ADVANCEMENT ACT.—In carrying out this section, the Secretary shall comply with section 12(d) of the National Technology Transfer and Advancement Act (15 U.S.C. 272 note).".

(b) TABLE OF CONTENTS AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by adding after the item relating to section 313 the following new item:

"Sec. 314. National standards for homeland security equipment and training.".

SEC. 3. 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) in subsection (b)(3), by striking "subsection (c)(2)" and inserting "subsection (e)(2)";

(2) 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 or other emergencies.";

(3) by redesignating subsection (c) as subsection (e); and

(4) by inserting after subsection (b) the following new subsections:

"(c) ELEMENTS OF THE TECHNOLOGY TRANSFER PROGRAM.—The activities of the program described in subsection (b)(6) shall include—

"(1) identifying available technologies that have been, or are in the process of being, developed, tested, evaluated, or demonstrated by the Department, other Federal agencies, the private sector, or foreign governments and international organizations, and reviewing whether such technologies may be useful in assisting Federal, State, and local governmental agencies, emergency response providers, or the private sector to prevent, prepare for, respond to, or recover from acts of terrorism or other emergencies; and

"(2) communicating to Federal, State, and local governmental agencies, emergency response providers, or the private sector the availability of such technologies, as well as the technology's specifications, satisfaction of appropriate standards, and the appropriate grants available from the Department to purchase such technologies.

"(d) RESPONSIBILITIES OF UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY.—In support of the activities described in subsection (c), the Under Secretary for Science and Technology shall—

"(1) conduct or support, based on the Department's current risk assessments, research, development, demonstrations, tests, and evaluations, as appropriate, of technologies identified under subsection (c)(1), including of—

"(A) any necessary modifications to such technologies for use by emergency response providers; and

"(B) incorporation of human factors in the development and suggested use of such technologies;

"(2) ensure that the technology transfer activities throughout the Directorate of Science and Technology are coordinated, including the technology transfer aspects of projects and grants awarded to the private sector and academia;

"(3) consult with the other Under Secretaries of the Department, the Director of the Federal Emergency Management Agency, and the Director of the Domestic Nuclear Detection Office on an ongoing basis;

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

"(5) consult with government agencies and standards development organizations as appropriate;

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

"(7) 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

"(8) 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) as appropriate, other organizations, other interested Federal, State, and local agencies, and other interested persons.".

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

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

SEC. 4. HOMELAND SECURITY SCIENCE AND TECHNOLOGY ADVISORY COMMITTEE.

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

"(j) TERMINATION.—The Department of Homeland Security Science and Technology Advisory Committee shall terminate 10 years after its establishment.".

SEC. 5. REGIONAL TECHNOLOGY INTEGRATION PROGRAM.

(a) AMENDMENT.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.) is amended by adding at the end the following:

"SEC. 315. REGIONAL TECHNOLOGY INTEGRATION PROGRAM.

"(a) IN GENERAL.—The Under Secretary for Science and Technology, in coordination with the Under Secretary for Preparedness, shall provide technical guidance, training, and other assistance, as appropriate, to support the transfer and integration of homeland security technologies and protocols in urban and other high risk jurisdictions determined by the Secretary to be at consistently high levels of risk from terrorist attack.

"(b) ACTIVITIES.—The program supported under subsection (a) shall work to—

"(1) facilitate the transition of innovative technologies and operational concepts, including those described in subsection (c);

"(2) integrate new technologies with existing infrastructure, systems, and concepts;

"(3) identify capability and technology gaps for future research, development, test, and evaluation;

"(4) evaluate system performance, life cycle, and human factor issues; and

"(5) disseminate lessons learned to other communities.

"(c) INNOVATIVE TECHNOLOGIES AND OPERATIONAL CONCEPTS.—The innovative technologies and operational concepts referred to in subsection (b)(1) include—

"(1) detection systems for weapons of mass destruction;

"(2) emergency management information systems;

"(3) situational awareness;

"(4) information sharing;

"(5) atmospheric transport and dispersion modeling;

"(6) public alerts and warnings;

"(7) aerial platforms; and

"(8) emergency medical support.

"(d) COORDINATION.—In setting priorities for and carrying out the activities under this section, the Under Secretary for Science and Technology shall consult and coordinate with appropriate governors, mayors, other State and local government officials, and first responders.".

(b) TABLE OF CONTENTS AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by adding after the item relating to section 314 the following new item:

"Sec. 315. Regional technology integration program.".

SEC. 6. CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) AMENDMENT.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et. seq.) is amended by adding at the end the following new section:

"SEC. 316. CYBERSECURITY RESEARCH AND DEVELOPMENT.

"(a) IN GENERAL.—The Under Secretary for Science and Technology shall support research and development, including fundamental, long-term research, in cybersecurity to improve the ability of the United States to prevent, protect against, detect, respond to, and recover from cyber attacks, with emphasis on research and development relevant to large-scale, high-impact attacks.

"(b) ACTIVITIES.—The research and development supported under subsection (a) shall include work to—

"(1) advance the development and accelerate the deployment of more secure versions of critical information systems, including—

"(A) fundamental Internet protocols and architectures, including for the domain name system and routing protocols; and

"(B) control systems used in critical infrastructure sectors;

"(2) improve and create technologies for detecting attacks or intrusions, including monitoring technologies;

"(3) improve and create mitigation and recovery methodologies, including techniques for containment of attacks and development of resilient networks and systems that degrade gracefully; and

"(4) develop and support infrastructure and tools to support cybersecurity research and development efforts, including modeling, testbeds, and data sets for assessment of new cybersecurity technologies.

"(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall coordinate activities with—

"(1) the Assistant Secretary for Cybersecurity and Telecommunications; and

"(2) other Federal agencies, including the National Science Foundation, the Defense Advanced Research Projects Agency, the Information Assurance Directorate of the National Security Agency, and the National Institute of Standards and Technology, to identify unmet needs and cooperatively support activities, as appropriate.

"(d) NATURE OF RESEARCH.—Activities under this section shall be carried out in accordance with section 306(a) of this Act.

"(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section such sums as may be necessary for fiscal year 2007.".

(b) TABLE OF CONTENTS AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by adding after the item relating to section 315 the following new item:

"Sec. 316. Cybersecurity research and development.".

SEC. 7. STANDARDS FOR CRITICAL INFRASTRUCTURE INFORMATION SYSTEMS.

(a) AMENDMENT.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et. seq.) is amended by adding at the end the following new section:

"SEC. 317. STANDARDS FOR CRITICAL INFRASTRUCTURE INFORMATION SYSTEMS.

"(a) STANDARDS PROGRAM.—The Under Secretary for Science and Technology shall establish a program to support the development and promulgation of national voluntary consensus standards for requirements, performance testing, and user training with respect to critical infrastructure information systems.

"(b) PURPOSE.—The standards developed under subsection (a) shall be designed to assist State and local jurisdictions, including those in urban and other areas at consistently high levels of risk from terrorist attack, and emergency response providers to acquire and implement critical infrastructure information systems and to store and access information regarding critical infrastructure to be used in responding to acts of terrorism or other emergencies.

"(c) REQUIREMENTS.—The standards developed under subsection (a) shall be designed to facilitate—

"(1) the interoperability of systems to enable sharing of information in a variety of formats and across stakeholders at the Federal, State, and local levels;

"(2) the ease of deployment of the systems to the field;

"(3) the ability to retrieve situational awareness information in real-time;

"(4) the integrity, security, and accessibility of stored information;

"(5) the application of human factors science in the development of the system;

"(6) the availability and content of training programs for potential users; and

"(7) meeting any other requirements determined by the Under Secretary to be appropriate.

"(d) REPORTS.—The Under Secretary for Science and Technology shall submit to Congress—

"(1) 6 months after the date of enactment of this section, a report describing the plan for carrying out the program under this section, which shall include a schedule for the development of national voluntary consensus standards for critical infrastructure information systems; and

"(2) 12 months after the date of enactment of this section, a report which shall include a description of—

"(A) the steps taken under this program and the funding dedicated to this program; and

"(B) the steps that have been or will be taken to promote the adoption of the standards by appropriate standard-setting organizations.

"(e) DEFINITIONS.—In this section—

"(1) the term 'critical infrastructure information systems' means software programs that store, manage, and display information about critical infrastructure to support situational awareness and real-time decisionmaking of law enforcement, fire services, emergency medical services, emergency management agencies, other emergency response providers, and critical infrastructure facility stakeholders. Critical infrastructure information may include maps and other geospatial information, emergency plans, interior and exterior imagery, entry and exit points, and any other information about infrastructure or facilities that may be beneficial to users of critical infrastructure information systems; and

"(2) the term 'critical infrastructure' has the meaning given that term in section 1016(e) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (42 U.S.C. 5195c(e)).".

(b) TABLE OF CONTENTS AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by adding after the item relating to section 316 the following new item:

"Sec. 317. Standards for critical infrastructure information systems.".

SEC. 8. SCHOLARSHIP AND FELLOWSHIP PROGRAMS AT THE DEPARTMENT OF HOMELAND SECURITY.

(a) IN GENERAL.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et. seq.) is amended by adding at the end the following new section:

"SEC. 318. SCHOLARSHIP AND FELLOWSHIP PROGRAMS.

"(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, shall encourage the development of an adequate supply of people trained in and performing research in science, technology, engineering, and mathematical fields relevant to homeland security.

"(b) RESPONSIBILITIES.—In carrying out this section, the Secretary may support—

"(1) programs at the undergraduate, graduate, and postdoctoral levels, including at Historically Black Colleges and Universities that are Part B institutions as defined in section 322(2) of the Higher Education Act of 1965 (20 U.S.C. 1061(2)) and minority institutions (as defined in section 365(3) of that Act (20 U.S.C. 1067k(3))); and

"(2) internship programs that take advantage of the homeland security research infrastructure available to the Department, including laboratories owned or operated by the Department, the Department of Energy National Laboratories, and University Centers of Excellence.".

(b) TABLE OF CONTENTS AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by adding after the item relating to section 317 the following new item:

"Sec. 318. Scholarship and fellowship programs.".

SEC. 9. REPORTS AND DEMONSTRATION PROJECT ON SURVEILLANCE CAMERA PROGRAMS.

(a) INVENTORY OF SURVEILLANCE SYSTEMS.—Not later than 120 days after the date of enactment of this Act, the Under Secretary for Science and Technology, in consultation with the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties, shall transmit a report to Congress on existing visual surveillance systems supported or utilized by the Department of Homeland Security. The report shall, for each system—

(1) describe the goals of the system, such as terrorism prevention, emergency response, and law enforcement;

(2) describe any potential uses of the system beyond its stated goals and if the system has been used in any of those ways;

(3) describe the rules governing how visual information generated by the system is collected, stored, analyzed, and disseminated; and

(4) describe the role of Federal, State, and local governments and private entities in the operation of the system and use of the data generated by the system.

(b) SYSTEMS COVERED.—The visual surveillance systems covered in the report required under subsection (a) shall include all systems for which—

(1) the Department provided funds for development, procurement, or implementation of the system; or

(2) the Department has access to the data gathered through the system.

(c) EVALUATION OF SURVEILLANCE SYSTEMS.—Not later than 1 year after the transmittal of the report under subsection (a), the Under Secretary for Science and Technology, in consultation with the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties, shall transmit a report to Congress evaluating the use and effectiveness of existing visual surveillance systems supported or utilized by the Department of Homeland Security. The report shall, for at least 6 systems that are representative of the systems listed in the report under subsection (a)—

(1) evaluate the effectiveness of the system in meeting its stated goals;

(2) review the privacy policies and implications of the system;

(3) review the civil rights and civil liberties policies and implications of the system;

(4) describe any lessons learned from the implementation of the system; and

(5) describe any remaining questions about the effectiveness and the privacy and civil liberties implications of such systems that cannot be addressed by this evaluation of surveillance systems and that may require demonstration programs to study.

(d) DEMONSTRATION PROJECT.—

(1) IN GENERAL.—Not sooner than 120 days after the transmittal of the report required under subsection (c), and based on the results of that evaluation, the Under Secretary for Science and Technology, in consultation with the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security, may establish a demonstration project to assess the effectiveness and the privacy and civil liberties implications of utilizing visual surveillance systems to enhance homeland security.

(2) BEST PRACTICES.—The demonstration project established under paragraph (1) shall thoroughly consider and incorporate best practices from within the United States and abroad, including from the United Kingdom, Israel, Canada, and Australia.

(3) MASS TRANSIT SECURITY.—If visual surveillance of a mass transit facility is included in the demonstration project under paragraph (1), the Under Secretary for Science and Technology shall consult with the Assistant Secretary for the Transportation Security Administration and shall ensure that the goals of the demonstration project are consistent with the research and development requirements of the National Strategy for Transportation Security.

(e) DEFINITION.—In this section, the term "visual surveillance" means the use of recording devices with the capability to obtain, store, or analyze video or static images, with the exception of data gathered via satellite systems.

SEC. 10. PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES IN TECHNOLOGY DEVELOPMENT.

(a) IN GENERAL.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et. seq.) is amended by adding at the end the following new section:

"SEC. 319. PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES IN TECHNOLOGY DEVELOPMENT.

"Not later than 180 days after the date of enactment of this section, the Under Secretary for Science and Technology, the Chief Privacy Officer, and the Officer for Civil Rights and Civil Liberties shall transmit to Congress a joint plan for how privacy and civil rights and civil liberties issues will be considered in technology research and development programs at the Department, including how such issues will be taken into account in defining requirements for technology performance and use of technologies in pilot programs.".

(b) TABLE OF CONTENTS AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by adding after the item relating to section 318 the following new item:

"Sec. 319. Privacy and civil rights and civil liberties issues in technology development.".

SEC. 11. SCIENCE AND TECHNOLOGY STRATEGIC PLAN.

(a) STRATEGIC PLAN.—Not later than 180 days after the date of enactment of this Act, the Under Secretary for Science and Technology shall transmit to Congress a strategic plan for the science and technology activities of the Department of Homeland Security. The plan shall include—

(1) statement of the overall mission of the Science and Technology Directorate;

(2) a prioritized list of objectives and the specific capabilities, including technologies and associated protocols, expertise, and facilities, needed to meet these objectives;

(3) a description of the processes and risk-based methodologies used to prioritize these objectives;

(4) a list of activities, including any long-term basic research programs, that the Under Secretary for Science and Technology will carry out to meet these objectives and develop the specific capabilities described under paragraph (2);

(5) a description of the metrics to be used for annual review of the activities;

(6) a description of all related programs and activities, within the Department or at other Federal agencies, with which the activities will be coordinated; and

(7) a description of the processes used to ensure that factors associated with manpower and infrastructure are considered during technology development.

(b) REGULAR UPDATING.—At the end of the fiscal year that occurs 5 years after the date of enactment of this Act, and every 5 years thereafter, the Under Secretary for Science and Technology shall transmit to Congress an update of this strategic plan.

SEC. 12. REPORTS TO CONGRESS ON SOCIAL AND BEHAVIORAL RESEARCH FOR HOMELAND SECURITY.

(a) REPORT ON THE USE OF SOCIAL AND BEHAVIORAL RESEARCH.—Not later than 1 year after the date of enactment of this Act, the Secretary of Homeland Security shall transmit to Congress a report on the Department's use of social and behavioral research, including—

(1) a compilation of the instances in which the Department has made use of—

(A) social and behavioral research in Department programs in preparedness and response, including risk communication activities, response plans, and training and guidance for decisionmakers;

(B) social and behavioral research, including human factors research, in Department technology development and acquisition programs;

(C) social and behavioral research in development of Department programs for informing the general public on how to prepare for, protect against, respond to, and mitigate the effects, both physical and psychological, of acts of terrorism, natural disasters, or other emergencies; and

(D) social and behavioral research regarding emergency preparedness and response, search and rescue, evacuation, and sheltering-in-place procedures for populations with special needs, including persons with disabilities, health problems, language barriers, and income barriers, the elderly, and children in relevant Department programs;

(2) specific citations or references to the social and behavioral research on which the Department has relied; and

(3) a plan for how the Department will ensure greater incorporation of social and behavioral research in program and communication activities in the near and long term.

(b) REPORT ON GAPS IN NEEDED SOCIAL AND BEHAVIORAL RESEARCH.—Not later than 180 days after the transmittal of the report under subsection (a), the Under Secretary for Science and Technology shall transmit to Congress a report identifying any gaps in the social and behavioral research needed to support the Department's mission, and providing a plan to address such gaps.

(c) CONSULTATION.—In preparing the reports under subsections (a) and (b), the Secretary and the Under Secretary for Science and Technology shall consult with other government agencies supporting social and behavioral research and nongovernmental experts in these fields.

SEC. 13. GUIDE FOR RESEARCHERS ON THE HOMELAND SECURITY IMPLICATIONS OF RESEARCH.

(a) IN GENERAL.—The Under Secretary for Science and Technology shall enter into an arrangement with the National Research Council of the National Academy of Sciences to prepare a guide for researchers to raise awareness in the scientific community about potential homeland security implications of their work and how laws and regulations apply to such research.

(b) TOPICS.—The topics covered in the guide prepared under subsection (a) shall include—

(1) international conventions;

(2) United States statutes, regulations, and guidelines, including those covering biological materials;

(3) the potential for legitimate research to be misused;

(4) responsibilities of the scientific community to reduce opportunities for misuse;

(5) case studies and examples; and

(6) any other topics determined by the Under Secretary for Science and Technology to be appropriate.

(c) DISSEMINATION.—The Under Secretary for Science and Technology shall transmit the guide prepared by the National Research Council under this section to Congress within 1 year of the date of enactment of this Act, and shall encourage the distribution of the guide throughout the homeland security and life sciences research communities, especially to students.

SEC. 14. PROJECT 25 STANDARDS COMPLIANCE.

The Under Secretary for Science and Technology, working with the Director of the National Institute of Standards and Technology and other appropriate Federal agencies, shall support assessment of compliance of first responder communications equipment with the Project 25 standards established by the Association of Public Safety Communications Officials International. The results of such assessments shall be made publicly available, in a manner to best assist first responder agencies in selecting such equipment.

SEC. 15. RAIL SECURITY RESEARCH AND DEVELOPMENT.

(a) ESTABLISHMENT OF RESEARCH AND DEVELOPMENT PROGRAM.—The Secretary of Homeland Security, through the Under Secretary for Science and Technology, in coordination with the Assistant Secretary of Homeland Security (Transportation Security Administration) and the Departmental Privacy Officer, and in consultation with the Secretary of Transportation, shall carry out a research and development program for the purpose of improving rail and mass transit security that may include research and development projects to—

(1) reduce the vulnerability of passenger trains, stations, and equipment to explosives and hazardous chemical, biological, and radioactive substances;

(2) test new emergency response and recovery techniques and technologies;

(3) develop improved freight technologies, including—

(A) technologies for sealing rail cars;

(B) automatic inspection of rail cars;

(C) communication-based train controls;

(D) signal system integrity at switches;

(E) emergency response training including training in a tunnel environment;

(F) security and redundancy for critical communications, electrical power, computer, and train control systems; and

(G) technologies for securing bridges and tunnels;

(4) test wayside detectors that can detect tampering with railroad equipment;

(5) support enhanced security for the transportation of hazardous materials by rail;

(6) mitigate damages in the event of a cyber attack; and

(7) address other vulnerabilities and risks identified by the Secretary.

(b) COORDINATION WITH OTHER RESEARCH INITIATIVES.—The Secretary of Homeland Security shall ensure that the research and development program authorized by this section is consistent with the National Strategy for Transportation Security and the Transportation Sector Specific Plan, and shall to the greatest extent possible leverage other ongoing research and development security related initiatives at the National Academy of Sciences; the Department of Homeland Security; the Department of Transportation, including University Transportation Centers and other institutes, centers, and simulators funded by the Department of Transportation; the Technical Support Working Group; other Federal agencies; and other Federal and private research laboratories and research entities with the capability to conduct both practical and theoretical research and technical systems analysis.

(c) PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES.—In carrying out research and development projects under this section, the Under Secretary for Science and Technology shall consult with the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties as appropriate and in accordance with the plan required by section 319 of the Homeland Security Act of 2002. Pursuant to sections 222 and 705 of the Homeland Security Act of 2002, the Chief Privacy Officer shall conduct privacy impact assessments and the Officer for Civil Rights and Civil Liberties shall conduct reviews, as appropriate, for research and development initiatives developed pursuant to this section.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary of Homeland Security to carry out this section such sums as may be necessary for each of fiscal years 2007 through 2009. Amounts made available pursuant to this subsection shall remain available until expended.

PURPOSE AND SUMMARY

The purpose of H.R. 4941 is to reform the science and technology programs and activities of the Department of Homeland Security (Department), and for other purposes. Specifically, this bill would reform the Department's Directorate of Science and Technology to enhance the Federal government's ability to research, develop, test, and evaluate innovative and emerging homeland security technologies that will help our Nation's emergency response providers and others prevent, prepare for, respond to, recover from, and mitigate against acts of terrorism and other emergencies.

BACKGROUND AND NEED FOR LEGISLATION

Until Congress and the Administration established the Department of Homeland Security's (Department) Directorate of Science and Technology (S&T Directorate) under the Homeland Security Act of 2002 (P.L. 107–296) (HSA), there had never been a "dedicated" research, development, testing, and evaluation system for emergency response providers. Under the HSA, the S&T Directorate's responsibilities include: "establishing priorities for, directing, funding, and conducting national research, development, test and evaluation, and procurement of technology and systems for . . . detecting, preventing, protecting against, and responding to, terrorist attacks," and "establishing a system for transferring homeland security developments or technologies to Federal, State, local government and private sector entities." Thus, the S&T Directorate's primary mission is to develop and disseminate technologies that enable emergency response providers and others to protect and secure our Nation.

Unlike most of the Department's other components, such as the Federal Emergency Management Agency, the Coast Guard, or the U.S. Secret Service, the S&T Directorate is not a legacy agency. Its establishment in March 2003, therefore, was a watershed event for our Nation. Yet, given the relative newness of the S&T Directorate, it has—not surprisingly—encountered more than the usual growing pains. Indeed, during the past three years, Congress has grown increasingly frustrated with the S&T Directorate's performance. The litany of complaints is long. The S&T Directorate has been criticized for: (1) a lack of transparent, strategic planning; (2) providing inadequate detail in its budget justifications; (3) systemic deficiencies in its financial and accounting controls; (4) poor response to the needs of its customers and end-users; and (5) failing to more rapidly develop and adopt currently existing defense technologies for homeland security purposes. Whether real or perceived, these and other problems caused many in Congress and elsewhere to lose confidence in the S&T Directorate's ability to fulfill its statutory responsibilities.

The Committee believes that technology can be the difference between victory and defeat in the global war on terror. As the terrorism threats to our Nation evolve, so must our technology. Technology is a force-multiplier, supporting the efforts of emergency re-

sponse providers to, among other things, detect weapons of mass destruction, communicate information, patrol our borders, and inspect our cargo. H.R. 4941 is intended to enhance the S&T Directorate's effectiveness and ensure that our Nation maintains its scientific and technological advantage over determined adversaries.

HEARINGS

On Thursday, July 21, 2005, the Subcommittee on Emergency Preparedness, Science, and Technology held a joint hearing with the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the Committee on Armed Services entitled "Technology Transfer: Leveraging Military Technology to Enhance Homeland Security." The Subcommittees received testimony from Ms. Sue Payton, Deputy Under Secretary of Defense for Advanced Systems and Concepts, Department of Defense; Dr. Tony Tether, Director, Defense Advanced Research Projects Agency, Department of Defense; Dr. John Kubricky, Director, Office of Systems Engineering and Development, Science and Technology Directorate, Department of Homeland Security; and Mr. Peter F. Verga, Principal Deputy Assistant Secretary of Defense for Homeland Defense, Department of Defense.

COMMITTEE CONSIDERATION

H.R. 4941 was introduced by Mr. Reichert, and Mr. Pascrell on March 14, 2006, and referred solely to the Committee on Homeland Security. On March 15, 2006, H.R. 4941 was referred to the Subcommittee on Emergency Preparedness, Science, and Technology.

On March 15, 2006, the Subcommittee on Emergency Preparedness, Science, and Technology met in open markup session and forwarded H.R. 4941 favorably to the Full Committee amended, by voice vote.

On June 14, 2006, the Full Committee met in open markup session and favorably ordered H.R. 4941 reported to the House, amended, by voice vote.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto.

On June 14, 2006, the Full Committee met in open markup session and favorably ordered H.R. 4941 reported to the House, amended, by voice vote.

The Committee considered a Committee Print showing the text of H.R. 4941, as Amended by the Subcommittee on Emergency Preparedness, Science, and Technology on March 15, 2006.

The following amendments were offered:

An Amendment in the Nature of a Substitute (#1) offered by Mr. King; was AGREED TO, without amendment, by voice vote.

A unanimous consent request to consider the Amendment in the Nature of a Substitute as base text for purposes of amendment, was not objected to.

An amendment offered by Ms. Sanchez to the Amendment in the Nature of a Substitute offered by Mr. King (#1A); in section 6, in the proposed section 316(e) of the Homeland Security Act of 2002,

strike "such sums as may be necessary" and insert "$50,000,000".; was not agreed to by a record vote of 13 yeas and 15 nays (Rollcall Vote No. 37).

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

Date: Wednesday, June 14, 2006 Convened: 10:09 a.m.

Adjourned: 11:10 a.m.

Meeting on : Markup of H.R. 4941, Homeland Security Science and Technology Enhancement Act of 2006

On agreeing to the amendment offered by Ms. Sanchez, #1A

☐ Attendance ☒ Recorded Vote Vote Number: 37 Total: Yeas 13 Nays 15

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska				*Mr. Bennie G. Thompson* *Mississippi, Ranking Member*	✓		
Mr. Lamar S. Smith Texas		✓		*Ms. Loretta Sanchez* *California*	✓		
Mr. Curt Weldon Pennsylvania		✓		*Mr. Edward J. Markey* *Massachusetts*			
Mr. Christopher Shays Connecticut		✓		*Mr. Norman D. Dicks* *Washington*	✓		
Mr. John Linder Georgia		✓		*Ms. Jane Harman* *California*	✓		
Mr. Mark E. Souder Indiana		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Tom Davis Virginia				*Ms. Nita M. Lowey* *New York*	✓		
Mr. Daniel E. Lungren California		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*	✓		
Mr. Jim Gibbons Nevada		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Rob Simmons Connecticut		✓		*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Mike Rogers Alabama		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Ms. Katherine Harris Florida		✓		*Mr. Bob Etheridge* *North Carolina*	✓		
Mr. Bobby Jindal Louisiana				*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Dave Reichert Washington				*Mr. Kendrick Meek* *Florida*	✓		
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Ms. Ginny Brown-Waite Florida		✓					
Mr. Peter T. King New York Chairman		✓		Total	**13**	**15**	

An amendment offered by Ms. Lowey to the Amendment in the Nature of a Substitute offered by Mr. King (#1B); at the end of the bill, add the following new section entitled "Sec. 14. Project 25 Standards Compliance."; was agreed to by voice vote.

An amendment offered by Ms. Norton to the Amendment in the Nature of a Substitute offered by Mr. King (#1C); at the end of the bill, add a new section entitled "Sec. 14. Rail Security Research and Development."; was agreed to, as amended, by voice vote.

An amendment offered by Mr. Shays to the amendment offered by Ms. Norton to the Amendment in the Nature of a Substitute offered by Mr. King (#1C1); in the authorization of appropriations subsection, strike paragraphs (1) through (3) and insert "such sums as may be necessary for each of fiscal years 2007 through 2009".; was agreed to by a record vote of 15 yeas and 13 nays (Rollcall Vote No. 36).

COMMITTEE ON HOMELAND SECURITY

U.S. House of Representatives

Date: Wednesday, June 14, 2006 Convened: 10:09 a.m.

Adjourned: 11:10 a.m.

Meeting on : Markup of H.R. 4941, Homeland Security Science and Technology Enhancement Act of 2006

On agreeing to the amendment offered by Mr. Shays, (#1(C)(1)) to the amendment offered by Ms. Norton (#1(C)) to the Amendment in the Nature of a Substitute (#1)

☐ Attendance ☒ Recorded Vote Vote Number: 36 Total: Yeas 15 Nays 15

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska				*Mr. Bennie G. Thompson* *Mississippi, Ranking Member*		✓	
Mr. Lamar S. Smith Texas	✓			*Ms. Loretta Sanchez* *California*		✓	
Mr. Curt Weldon Pennsylvania	✓			*Mr. Edward J. Markey* *Massachusetts*			
Mr. Christopher Shays Connecticut	✓			*Mr. Norman D. Dicks* *Washington*		✓	
Mr. John Linder Georgia	✓			*Ms. Jane Harman* *California*		✓	
Mr. Mark E. Souder Indiana	✓			*Mr. Peter A. DeFazio* *Oregon*		✓	
Mr. Tom Davis Virginia				*Ms. Nita M. Lowey* *New York*		✓	
Mr. Daniel E. Lungren California	✓			*Ms. Eleanor Holmes Norton* *District of Columbia*		✓	
Mr. Jim Gibbons Nevada	✓			*Ms. Zoe Lofgren* *California*		✓	
Mr. Rob Simmons Connecticut	✓			*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Mike Rogers Alabama	✓			*Mr. Bill Pascrell, Jr.* *New Jersey*		✓	
Mr. Stevan Pearce New Mexico	✓			*Mrs. Donna M. Christensen* *U.S. Virgin Islands*		✓	
Ms. Katherine Harris Florida	✓			*Mr. Bob Etheridge* *North Carolina*		✓	
Mr. Bobby Jindal Louisiana				*Mr. James R. Langevin* *Rhode Island*		✓	
Mr. Dave Reichert Washington				*Mr. Kendrick Meek* *Florida*		✓	
Mr. Michael McCaul Texas	✓						
Mr. Charlie Dent Pennsylvania	✓						
Ms. Ginny Brown-Waite Florida	✓						
Mr. Peter T. King New York Chairman	✓			Total	**15**	**13**	

An amendment offered by Mrs. Lowey to the Amendment in the Nature of a Substitute offered by Mr. King (#1C); at the end of the bill, add a new section entitled "Sec. 14. Grant Funding Allocations."; was withdrawn by unanimous consent.

On May 15, 2006, the Subcommittee on Emergency Preparedness, Science, and Technology met in open markup session and favorably forwarded H.R. 4941 to the Full Committee for consideration, amended, by voice vote.

The following amendments were offered:

An amendment offered by Mrs. Lowey (#1) to H.R. 4941; at the end of the bill, insert a new section entitled "National Strategy for Interoperable Communications."; was withdrawn by unanimous consent.

An amendment offered by Mr. Thompson (#2) to H.R. 4941; at the appropriate place in the bill, insert the following new section entitled "Special Needs and Disabilities Research Center."; was withdrawn by unanimous consent.

An amendment offered by Ms. Norton (#3) to H.R. 4941; at the end of the bill, insert a new section entitled "Rail Security Research and Development."; was not agreed to, as amended, by a recorded vote of 5 yeas and 7 nays (Rollcall Vote No. 1).

A unanimous consent request by Ms. Norton to amend her amendment (#3) to H.R. 4941 on Page 1, line 10, to strike "and" and insert "rail,"; Page 1, line 11 to insert after "rail" ", and rail transit"; was not objected to.

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

SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, SCIENCE AND TECHNOLOGY

Date: March 15, 2006 Convened: _____

Adjourned: _____

Meeting on : Markup of H.R. 4941, "Homeland Security Science and Technology Enhancement Act of 2006." Amendment offered by Ms. Norton (#3), as amended.

☐ Attendance ☒Recorded Vote Vote Number: 1 Total: Yeas 5 Nays 7

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Lamar Smith Texas				*Mr. Bill Pascrell, Jr.* *New Jersey*	✔		
Mr. Curt Weldon Pennsylvania		✔		*Ms. Loretta Sanchez* *California*			
Mr. Rob Simmons Connecticut				*Mr. Norman D. Dicks* *Washington*	✔		
Mr. Mike Rogers Alabama				*Ms. Jane Harman* *California*			
Mr. Stevan Pearce New Mexico		✔		*Ms. Nita M. Lowey* *New York*			
Ms. Katherine Harris Florida				*Ms. Eleanor Holmes Norton* *District of Columbia*	✔		
Mr. Michael McCaul Texas		✔		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*			
Mr. Charlie Dent Pennsylvania		✔		*Mr. Bob Etheridge* *North Carolina*	✔		
Ms. Ginny Brown-Waite Florida		✔					
				Mr. Bennie G. Thompson *Mississippi, (Ex Officio)*	✔		
Mr. Peter T. King New York, (Ex Officio)		✔					
Mr. Dave Reichert Washington, Chairman		✔					
				Total	5	7	

An amendment offered by Ms. Sanchez (#4) to H.R. 4941, in the proposed section 316 of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.), as added by section 7 of the bill, add the following new section entitled "Authorization of Appropriations."; was AGREED TO, amended, by voice vote.

An amendment offered by Mr. McCaul (#4A) to the amendment offered by Ms. Sanchez (#4) to H.R. 4941, on Page 1, line 3, strike "$50,000,000" and insert "such sums as may be necessary".; was agreed to by a recorded vote of 7 yeas and 5 nays (Rollcall Vote No. 2).

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

SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, SCIENCE AND TECHNOLOGY

Date: March 15, 2006 Convened: _____

Adjourned: _____

Meeting on : Markup of H.R. 4941, "Homeland Security Science and Technology Enhancement Act of 2006." Amendment offered by Mr. McCaul (#4A)to the amendment offered by Ms. Norton

☐ Attendance ☒ Recorded Vote Vote Number: 2 Total: Yeas 5 Nays 7

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Lamar Smith Texas				*Mr. Bill Pascrell, Jr.* *New Jersey*		✔	
Mr. Curt Weldon Pennsylvania	✔			*Ms. Loretta Sanchez* *California*			
Mr. Rob Simmons Connecticut				*Mr. Norman D. Dicks* *Washington*		✔	
Mr. Mike Rogers Alabama				*Ms. Jane Harman* *California*			
Mr. Stevan Pearce New Mexico	✔			*Ms. Nita M. Lowey* *New York*			
Ms. Katherine Harris Florida				*Ms. Eleanor Holmes Norton* *District of Columbia*		✔	
Mr. Michael McCaul Texas	✔			*Mrs. Donna M. Christensen* *U.S. Virgin Islands*			
Mr. Charlie Dent Pennsylvania	✔			*Mr. Bob Etheridge* *North Carolina*		✔	
Ms. Ginny Brown-Waite Florida	✔						
				Mr. Bennie G. Thompson *Mississippi, (Ex Officio)*		✔	
Mr. Peter T. King New York, (Ex Officio)	✔						
Mr. Dave Reichert Washington, Chairman	✔						
				Total	7	5	

An amendment offered by Ms. Sanchez (#5) to H.R. 4941; at the end of the bill, add the following new section entitled "Homeland Security Advanced Research Projects Agency Report."; was withdrawn by unanimous consent.

An amendment offered by Mr. Pascrell (#6) to H.R. 4941; at the end of the bill, insert a new section entitled "Report on Counter Man-Portable Air Defense System."; was WITHDRAWN by unanimous consent.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

H.R. 4941, the "Homeland Security Science and Technology Enhancement Act of 2006," is intended to enhance the ability of the Department of Homeland Security's (Department) Directorate of Science and Technology (S&T Directorate) to develop and disseminate technologies that will help our Nation's emergency response providers and other "end-users" prevent, prepare for, respond to, recover from, and mitigate against acts of terrorism and other emergencies. Among other things, this bill directs the Secretary of Homeland Security, acting through the Under Secretary for Science and Technology, to: develop a strategic plan for the Department's science and technology activities; support the development, promulgation, and updating of national voluntary consensus standards for equipment and training for emergency response providers and components of the Department; establish a technology development and transfer program to facilitate the identification, modification, and commercialization of promising homeland security technologies and equipment; establish a regional technology integration program to facilitate the transition of innovative technologies and operational concepts to urban and other high risk areas; support research and development, including fundamental, long-term research, in cybersecurity; and report to Congress on how the Department will consider privacy and civil rights and civil liberties issues in conducting its activities. H.R. 4941 provides the Department with additional legislative guidance to support its mission of ensuring that our Nation possesses the technology necessary to handle catastrophic incidents, especially those involving chemical, biological, radiological, nuclear, and explosive weapons.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 4941, the Homeland Security Science and Technology Enhancement Act of 2006, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 13, 2006.

Hon. PETER T. KING,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 4941, the Homeland Security Science and Technology Enhancement Act of 2006.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz.

Sincerely,

DONALD B. MARRON,
Acting Director.

Enclosure.

H.R. 4941—Homeland Security Science and Technology Enhancement Act of 2006

Summary: H.R. 4941 would authorize the appropriation of such sums as necessary for fiscal year 2007 through 2009 for the Department of Homeland Security (DHS) to carry out research and development programs to improve rail and mass transit security. The bill also would authorize the appropriation of sums necessary for fiscal year 2007 and DHS to support research and development programs to improve the security of information systems. Finally, the legislation would require DHS to prepare several reports and plans relating to the use of technology to enhance national security. CBO estimates that implementing H.R. 4941 would cost about $140 million over the 2007–2011 period, assuming appropriation of the necessary amounts. Enacting the bill would not affect direct spending or receipts.

H.R. 4941 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no cost on state, local, or tribal governments.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 4941 is shown in the following table. The costs of this legislation fall within budget function 750 (administration of justice).

	By fiscal year, in millions of dollars—				
	2007	2008	2009	2010	2011
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Estimated Authorization Level	58	40	40	0	0
Estimated Outlays	18	29	47	28	16

Basis of estimate: CBO estimates that implementing H.R. 4941 would cost about $140 million over the 2007–2011 period. For this estimate, CBO assumes that the necessary amounts will be appro-

priated near the start of each fiscal year and that spending will follow historical patterns for similar activities.

H.R. 4941 would authorize the appropriation of such sums as necessary for fiscal years 2007 through 2009 for DHS to carry out a research and development program to improve rail and mass transit security. Under the bill, this program would support technologies to protect bridges and tunnels, secure hazardous materials transported by rail, inspect rail cars and stations more thoroughly, and test emergency response and recovery operations. DHS is currently conducting a $10 million pilot program over 18 months to improve technologies that enhance the security of passenger rail operations. Based on the cost and scope of the pilot program, CBO expects that it would cost about $40 million annually over the 2007–2009 period to carry out the bill's research and development program.

The bill would authorize the appropriation of sums necessary for fiscal year 2007 for DHS to support research and development programs to improve the security of information systems. For fiscal year 2006, $16.7 million was appropriated for cybersecurity research and development programs in DHS. Based on that level of funding, CBO estimates that an authorization level of $17 million for 2007 would be sufficient to carry out this provision.

This legislation also would require DHS to prepare several reports and plans relating to the use of technology to enhance national security. Based on the costs of similar activities, CBO estimates that it would cost about $1 million in fiscal year 2007 to carry out those provisions.

Intergovernmental and private-sector impact: H.R. 4941 contains no intergovernmental or private-sector mandates as defined in UMRA and would not affect the budgets of state, local, or tribal governments.

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.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

COMPLIANCE WITH HOUSE RESOLUTION 1000

In compliance with H. Res. 1000, adopted on September 14, 2006, the Committee finds that H.R. 4941 does not provide authority, including budget authority, or recommend the exercise of authority, including budget authority, for a contract, loan, loan guarantee, grant, loan authority, or other expenditure with or to a non-Federal entity.

ADVISORY COMMITTEE STATEMENT

H.R. 4941 creates an advisory committee within the meaning of section 5(b) of the Federal Advisory Committee Act. Specifically, section 3 directs the Under Secretary for Science and Technology

of the Department of Homeland Security (Department), in coordination with the Secretary of Defense, to establish a working group to advise and assist the Department's Technology Clearinghouse in identifying military technologies with possible homeland security applications.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 1, which grants Congress the power to provide for the common Defense of the United States.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Sec 1. Short title

This section cites the measure as the "Homeland Security Science and Technology Enhancement Act of 2006."

Sec. 2. National standards for Homeland Security equipment and training

Subsection (a) requires the Secretary of Homeland Security (Secretary), acting through the Under Secretary for Science and Technology (Under Secretary), and in consultation with other components of the Department of Homeland Security (Department) and relevant public and private sector groups, to support developing, promulgating, and, as necessary, updating, national voluntary consensus standards for the performance, use, and validation of homeland security equipment. The standards for the performance, use, and validation of equipment should focus on maximizing interoperability, interchangeability, durability, flexibility, efficiency, portability, and safety. Standards should cover all appropriate uses of homeland security equipment by Federal, State, and local government and non-government emergency response providers, and Department personnel.

Grant applicants who seek to purchase or upgrade equipment with Federal funds must either buy items that meet these standards or explain why non-standard items will be superior. When an operational unit of the Department proposes to upgrade or purchase new equipment, the head of that unit shall consult with the Under Secretary on whether such equipment meets or exceeds any applicable national voluntary consensus standards and whether there is need for the Department to support the development or updating of applicable national voluntary consensus standards.

Subsection (b) also requires the Secretary, in consultation with the Under Secretary, other components of the Department, and relevant public and private sector groups, to support developing, promulgating, and, as necessary, updating, national voluntary con-

sensus standards for training that will enable Federal, State, and local government and non-government emergency response providers and Department personnel to use equipment effectively and appropriately in carrying out their missions.

The Secretary must coordinate with the Secretary of Health and Human Services and the Secretary of Transportation when developing any national voluntary consensus standards that involve or relate to equipment or training for emergency response providers that involve or relate to health or emergency medical services professionals, including emergency medical professionals.

The Committee stresses the importance of developing national voluntary consensus standards that are dynamic, and that will encourage a wide variety of creative, private sector-generated solutions to homeland security challenges. Appropriate national voluntary consensus standards will help private sector entities identify potential markets and their characteristics. To the extent that they do, they can serve as an indirect stimulus to economic growth, while ensuring that emergency response providers get the equipment and training most likely to help them prevent, prepare for, respond to, mitigate against, and recover from acts of terrorism, natural disasters, or other emergencies.

The Committee is also aware of numerous private and not-for-profit organizations working with State and local governments to implement emergency response provider equipment and training standards. The Secretary should consult with as many of these organizations as practicable in the development of the national voluntary consensus standards.

Sec. 3. Technology development and transfer

Subsection (a) directs the Secretary of Homeland Security (Secretary) to complete the establishment of the Technology Clearinghouse within the Directorate of Science and Technology (S&T Directorate), as called for in the Homeland Security Act of 2002 (P.L. 107–296) (HSA), no later than 90 days after the date of enactment.

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

- Conducting surveys and reviews of available technologies developed by the Department of Homeland Security (Department), other Federal agencies, the private sector, or foreign entities, for potential use for homeland security purposes;
- Conducting or supporting research and development (R&D) activities of technologies identified to be transferred for homeland security purposes;
- Communicating the availability, specifications, conformity to standards, and appropriate grants for the purchase, of such technologies to governmental agencies, first responders, and the private sector;
- Coordinating all technology transfer activities of the S&T Directorate, including projects and grants awarded to the private sector and academia;

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

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

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

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

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

The Committee notes that the Secretary, acting through the Under Secretary for Science and Technology (Under Secretary), must consult with the Department's other Under Secretaries and the Assistant Secretary for Grants and Training, with respect to this technology transfer program. The Committee encourages the Under Secretary to include the U.S. Fire Administration in its consultations. The Committee further recommends that the Department consider utilizing existing interagency entities, such as the Civil Applications Committee, when coordinating and entering into agreements with other Federal departments and agencies to facilitate effective commercialization of technologies.

This section's emphasis on the need for the Department to expedite the transfer of homeland security technologies to improve preparedness for acts of terrorism, does not suggest that the Department should ignore technology development and deployment in support of its important non-homeland security missions. The Department should continue to prioritize, maintain, and, where ap-

propriate, expand, technology development and transfer activities related to its other missions, including its trade and customs revenue functions under Section 412(b)(1) of the HSA.

Sec. 4. Homeland Security Science and Technology Advisory Committee

This section amends Section 311(j) of the Homeland Security Act of 2002 (P.L. 107–296) (HSA) by authorizing the Homeland Security Science and Technology Advisory Committee (HSSTAC) for a period of ten (10) years.

The HSSTAC's mission is to serve as a source of independent, scientific, and technical planning advice for the Under Secretary for Science and Technology. It meets at least four times a year, and includes Members with expertise in countermeasures to chemical, biological, radiological, nuclear and high explosive threats; critical infrastructure protection; borders and transportation security; intelligence; vulnerability analysis; systems engineering; and first response. Under the HSA, the Department of Homeland Security, must terminate the HSSTAC. The Committee strongly supports the work of the HSSTAC, and believes it is appropriate to extend HSSTAC for a period of up to ten (10) years from the effective date of the HSA.

Sec. 5. Regional Technology Integration Program

This section directs the Under Secretary of Science and Technology, in consultation with the Under Secretary for Preparedness and appropriate State and local government officials, to establish a regional technology integration program to support the transfer and integration of innovative homeland security technologies and operational concepts in urban and other high risk areas. This program shall work to: (1) facilitate the transition of innovative technologies and operational concepts, such as detection systems, emergency management information systems, and atmospheric transport and dispersion modeling; (2) integrate new technologies with existing infrastructure, systems, and concepts; (3) identify capability and technology gaps for future research, development, testing, and evaluation; (4) evaluate system performance, life cycle, and human factor issues; and (5) disseminate lessons learned to other communities.

This program will serve as the successor to the Directorate of Science and Technology's Regional Technology Integration (RTI) Initiative, a pilot program in four urban areas that tests maturing hardware and concepts, and provides information on how to best choose, deploy, and manage innovative and advanced technologies. Because of the RTI's success in those four urban areas, the Committee believes the Department of Homeland Security should replicate it in other high risk areas.

Sec. 6. Cybersecurity research and development

This section directs the Under Secretary for Science and Technology to support research and development, including fundamental, long-term research, of cybersecurity, to improve the ability of the United States to prevent, protect against, detect, respond to, and recover from cyber attacks. These efforts should emphasize re-

search and development relevant to large-scale, high-impact attacks.

The Committee is concerned that weaknesses in cybersecurity research and development have contributed significantly to the vulnerability of our Nation's information infrastructure. While a number of information technology companies support research and development of network security, security inadequacies cannot be addressed solely through short-term industry-based applied research. Our Nation's cybersecurity research and development enterprise clearly needs strengthening. Not only is too little research being conducted in this important area, but the research that this being performed is too incremental to lead to breakthroughs. The Committee, therefore, believes that the Directorate of Science and Technology should assume a leadership role in this area.

Sec. 7. Standards for critical infrastructure information systems

This section directs the Under Secretary for Science and Technology to establish a program to support the development and promulgation of national voluntary consensus standards for requirements, performance testing, and user training with respect to critical infrastructure information systems. Such standards will assist State and local areas and emergency response providers in acquiring and implementing such information systems and in storing and accessing information regarding critical infrastructure for use in responding to, and recovering from, emergencies.

Sec. 8. Scholarship and fellowship programs at the Department of Homeland Security

This section directs the Secretary of Homeland Security (Secretary), acting through the Under Secretary for Science and Technology, to encourage the development of an adequate supply of people trained and performing research in science, technology, engineering, and mathematical fields relevant to homeland security. The Secretary may support programs that utilize the Department of Homeland Security's (Department) research, development, testing, and evaluation infrastructure, including laboratories owned or operated by the Department, the Department of Energy's National Laboratories, and University Centers of Excellence. These programs may include undergraduate, graduate, and postdoctoral programs, including those at historically black colleges or universities, Hispanic-serving institutions, and tribally controlled colleges or universities, and internship programs.

The Committee is concerned about the size and quality of the national research community engaged in homeland security research. Our Nation's security depends on our ability to develop and produce innovative technologies. It is imperative, therefore, for the Department to help nurture the next generation of scientists as they study ways to prevent terrorist attacks within the U.S., reduce America's vulnerability to terrorism, and minimize the damage and recovery efforts from attacks that do occur. A robust DHS scholars and fellows program is an integral part of harnessing science in support of security.

Sec. 9. Reports on Surveillance Camera Demonstration Programs

This section directs the Under Secretary for Science and Technology (Under Secretary), in consultation with the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties, to submit a report to Congress, not later than 120 days after the date of enactment, on existing visual systems supported or utilized by the Department of Homeland Security (Department). The report, shall: (1) describe the goals of each system, such as terrorism prevention, emergency response, and law enforcement; (2) describe any potential uses of each system beyond its stated goals and if the system has been used in any of those ways; (3) describe the rules governing how visual information generated by each system is collected, stored, analyzed, and disseminated; and (4) describe the role of Federal, State, and local governments and private entities in the operation of each system and the use of the data each system generates. The report shall include all visual surveillance systems for which the Department provided funds for development, procurement, implementation, or for which the Department has access to the data gathered through the system.

Not later than one year after transmittal of the report described above, the Under Secretary, in consultation with the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties, must transmit a report to Congress evaluating the use and effectiveness of existing visual surveillance systems supported or utilized by the Department. The report shall: (1) evaluate the systems' effectiveness meeting its stated goals; (2) review the systems' privacy policies and implications; (3) review the systems' policies and implications for civil rights and civil liberties; (4) describe any lessons learned from the systems' implementation; and (5) describe any remaining questions about the systems' effectiveness and privacy and civil liberties implications that cannot be addressed by this evaluation and that may require demonstration programs to study.

Sec. 10. Privacy and civil rights and civil liberties issues in technology development

This section directs the Under Secretary for Science and Technology, the Chief Privacy Officer, and the Officer for Civil Rights and Civil Liberties to transmit to Congress, within 180 days of the date of enactment, a joint plan for how privacy, civil rights, and civil liberties issues will be considered in technology research and development programs at the Department of Homeland Security, including how such issues will be taken into account in defining requirements for technology performance and the use of technologies in pilot programs.

Sec. 11. Science and technology strategic plan

This section directs the Under Secretary for Science and Technology (Under Secretary) to transmit to Congress, not later than 180 days from the date of enactment, a strategic plan for the science and technology activities of the Department of Homeland Security. The plan shall include: (1) a prioritized list of objectives and the specific capabilities, including technologies and associated protocols, expertise, and facilities, needed to meet these objectives; (2) a description of the processes and risk-based methodologies used to prioritize these objectives; (3) a list of activities, including

any long-term basic research programs, that the Under Secretary will carry out to meet these objectives; (4) a description of the metrics to be used for annual review of the activities; and (5) a description of all related programs and activities, within the Department or at other Federal departments or agencies, with which the activities will be coordinated. Thereafter, the Under Secretary shall update this strategic plan every five years.

The Committee expects that the strategic plan, in providing a description of objectives for the science and technology programs of the Department, will also describe capabilities needed to meet these objectives. Such capabilities would include not only technologies (such as equipment, sensors, and software) but also the associated resources needed to implement technologies effectively, such as training programs for first responders, concepts of operation for responses to incidents, technical information reach-back resources, national voluntary consensus standards development, and specialized facilities for testing.

Sec. 12. Reports to Congress on social and behavioral research for homeland security

This section directs the Secretary of Homeland Security to transmit to Congress, not later than one year after the date of enactment, a report on the Department's use of social and behavioral research. This report shall include a compilation of the instances in which the Department of Homeland Security (Department) has made use of: (1) social and behavioral research in Departmental programs for preparedness and response, including risk communication activities, response plans, and training and guidance for decision makers; (2) social and behavioral research, including human factors research, in Department technology development and acquisition programs; (3) social and behavioral research in development of programs for informing the public of how to prepare for, protect against, respond to, and mitigate the effects of acts of terrorism, natural disasters, and other emergencies; and (4) social and behavioral research regarding emergency preparedness and response, search and rescue, evacuation, and sheltering-in-place procedures for populations with special needs, including persons with disabilities, health problems, language barriers, and income barriers; the elderly; and children. The report should also include specific citations or references to the social and behavioral research the Department has relied on; and a plan for how the Department will ensure greater incorporation of social and behavioral research in program and communication activities in the near- and long-term.

Not later than 180 days after the transmittal of the report described above, the Under Secretary for Science and Technology (Under Secretary) shall transmit to Congress a report identifying any gaps in the social and behavioral research needed to support the Department's mission, and a plan to address such gaps. In preparing these reports, the Secretary and the Under Secretary shall consult with other Federal departments or agencies supporting social and behavioral research, and non-governmental experts in these fields.

The Committee is concerned about Departmental programs not incorporating the results of social and behavioral research. Re-

search in these fields has a key role to play in optimizing public communication materials and response planning, and developing effective user interfaces in technical equipment. For example, although there is a wealth of social and behavioral research that could be utilized to optimize communication of essential information to the public, it is not utilized in communication materials produced by the Department's public affairs office. Incorporating social and behavioral research into Departmental activities, programs, and products is an important element of improving our Nation's readiness, and is consistent with the Directorate of Science and Technology's role of providing scientific support to the components of the Department.

Sec. 13. Guide for researchers on the homeland security implications of research

This section directs the Under Secretary for Science and Technology (Under Secretary) to enter into an arrangement with the National Research Council of the National Academy of Sciences to prepare a guide for researchers to raise the scientific community's awareness of potential homeland security implications of their work, and how laws and regulations apply to such research. The guide should include: (1) international conventions; (2) U.S. statutes, regulations, and guidelines, including those covering biological materials; (3) the potential for legitimate research to be misused; (4) the scientific community's responsibilities to reduce opportunities for misuse; (5) case studies and examples; and (6) any other topics the Under Secretary determines are appropriate.

The Under Secretary shall transmit the guide developed under this section to Congress within one year of the date of enactment, and encourage distribution of the guide throughout the homeland security and life sciences research communities, especially to students.

The Committee notes that the National Research Council publishes "On Being a Scientist: Responsible Conduct in Research," a guide for instructing scientists on their responsibility to ensure the scientific integrity of their work and that of their colleagues. This guide, last revised in 1995, covers a breadth of ethical, personal, and professional issues that could be encountered in research environments. Over 350,000 copies of this guide have been sold and it has been translated into four languages. This guide can serve either as a model or a vehicle (in an updated third edition) for addressing issues related to homeland security.

Over the last several years, the responsible conduct of research has received significant attention from the scientific community itself and through professional associations, the National Academy of Sciences, and editorials. The U.S. Government has also weighed in, with the greatest scrutiny and debate focused on life sciences research. The National Research Council's report, "Biotechnology Research in an Age of Terrorism," recommended creating programs to educate scientists about the dual use dilemma in the life sciences. Another recommendation included the establishment of an Advisory Committee. The Department of Health and Human Services created the National Science Advisory Board for BioSecurity (Advisory Board), which held its first meeting June 2005. The Advisory Board has identified and begun to address a number of

issues relating to dual use research in the life sciences. The expeditious creation and wide dissemination of the guide described in this section would complement the Advisory Board's work in this area.

Sec. 14. Project 25 standards compliance

This section directs the Under Secretary for Science and Technology, in cooperation with the Director of the National Institute of Standards and Technology and other relevant Federal departments or agencies, to support measuring the compliance of emergency response providers' communications equipment with the Project 25 Standards (Project 25) established by the Association of Public Safety Communications Officials International. The results of these assessments shall be made publicly available, in a manner to best assist first responder agencies in selecting such equipment.

The Committee recognizes the utility of Project 25 in providing uniform standards for digital public safety radio communications equipment vital to seamless coordination and communication among emergency response providers. The Committee believes that the Directorate of Science and Technology should use Project 25 as an assessment tool to inform emergency response providers about the overall effectiveness and communications value of the technologies available to them. Publicly disseminating the Project 25 performance evaluations should ultimately give emergency response providers the real-world performance data they need to make informed technology acquisition decisions that meet the communications and security needs of communities, states, and the Nation.

Sec. 15. Rail Security Research and Development

This section directs the Secretary of Homeland Security (Secretary), through the Under Secretary for Science and Technology (Under Secretary), in coordination with the Assistant Secretary of Homeland Security for Transportation Security (Assistant Secretary) and the Department of Homeland Security's Privacy Officer, and in consultation with the Secretary of Transportation, to establish a research and development (R&D) program aimed at enhancing rail and mass transit security. Specifically, the R&D program shall include projects that: (1) reduce the vulnerability of passenger trains, stations, and equipment to explosives and hazardous chemical, biological, and radioactive agents; (2) test new emergency response and recovery techniques and technologies; (3) develop improved freight technologies; (4) test wayside detectors capable of detecting tampering with railroad equipment; (5) support enhanced security for rail transportation of hazardous materials; (6) mitigate damages in the event of a cyber attack; and (7) address other vulnerabilities and risks identified by the Secretary. This section authorizes such sums as may be necessary in each Fiscal Year 2007 through 2009 to carry out this R&D program.

The Secretary must ensure that the R&D program is consistent with the National Strategy for Transportation Security and the Transportation Sector Specific Plan and, to the greatest extent possible, leverages existing security-related research and development initiatives at the National Academy of Sciences, the Department of Homeland Security (Department), the Department of Transportation (including University Transportation Centers), the Technical

Support Working Group, other Federal agencies, and other Federal and private research laboratories and entities with the capability to conduct both practical and theoretical research and technical systems analysis.

In pursuing and carrying out the rail security R&D program authorized under this section, the Under Secretary must consult with the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties as appropriate, and in accordance with the plan established under Section 10. In addition, this section directs the Chief Privacy Officer to conduct privacy impact assessments and directs the Officer for Civil Rights and Civil Liberties to undertake reviews of the projects developed under this section.

The Committee notes that the R&D program developed under this section will provide the Department with a specialized research forum to develop and apply an array of promising, cutting-edge rail security technologies. The Committee also notes that this program is especially salient and necessary given the terrorist plot against the New York City transit system thwarted by law enforcement in July. This most recent plot against our Nation, combined with the deadly attacks on commuter train systems in Mumbai, Republic of India, on July 11, 2006, and in London, on July 7, 2005, demonstrate that rail infrastructure has security vulnerabilities and is an emerging terrorist target in the United States, and worldwide. The rail security R&D program is a substantive step toward responding to this dangerous trend through expanded research into technologies that will better secure our Nation's transportation lifelines and, in turn, better protect our citizens who depend on them daily.

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. 1. Short title; table of contents.

* * * * * * *

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

Sec. 301. Under Secretary for Science and Technology.

* * * * * * *

Sec. 314. National standards for homeland security equipment and training.
Sec. 315. Regional technology integration program.
Sec. 316. Cybersecurity research and development.
Sec. 317. Standards for critical infrastructure information systems.
Sec. 318. Scholarship and fellowship programs.

Sec. 319. Privacy and civil rights and civil liberties issues in technology development.

* * * * * * *

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

SEC. 311. HOMELAND SECURITY SCIENCE AND TECHNOLOGY ADVISORY COMMITTEE.

(a) * * *

* * * * * * *

[(j) TERMINATION.—The Department of Homeland Security Science and Technology Advisory Committee shall terminate 3 years after the effective date of this Act.]

(j) TERMINATION.—The Department of Homeland Security Science and Technology Advisory Committee shall terminate 10 years after its establishment.

* * * * * * *

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) * * *

* * * * * * *

(3) The establishment of a technical assistance team to assist in screening, as appropriate, proposals submitted to the Secretary (except as provided in subsection [(c)(2)] *(e)(2)*) to assess the feasibility, scientific and technical merits, and estimated cost of such proposals, as appropriate.

* * * * * * *

(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 or other emergencies.

(c) ELEMENTS OF THE TECHNOLOGY TRANSFER PROGRAM.—The activities of the program described in subsection (b)(6) shall include—

(1) identifying available technologies that have been, or are in the process of being, developed, tested, evaluated, or demonstrated by the Department, other Federal agencies, the private sector, or foreign governments and international organizations, and reviewing whether such technologies may be useful in assisting Federal, State, and local governmental agencies, emergency response providers, or the private sector to prevent, prepare for, respond to, or recover from acts of terrorism or other emergencies; and

(2) communicating to Federal, State, and local governmental agencies, emergency response providers, or the private sector the availability of such technologies, as well as the technology's specifications, satisfaction of appropriate standards, and the appropriate grants available from the Department to purchase such technologies.

(d) RESPONSIBILITIES OF UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY.—In support of the activities described in subsection (c), the Under Secretary for Science and Technology shall—

(1) conduct or support, based on the Department's current risk assessments, research, development, demonstrations, tests, and evaluations, as appropriate, of technologies identified under subsection (c)(1), including of—

(A) any necessary modifications to such technologies for use by emergency response providers; and

(B) incorporation of human factors in the development and suggested use of such technologies;

(2) ensure that the technology transfer activities throughout the Directorate of Science and Technology are coordinated, including the technology transfer aspects of projects and grants awarded to the private sector and academia;

(3) consult with the other Under Secretaries of the Department, the Director of the Federal Emergency Management Agency, and the Director of the Domestic Nuclear Detection Office on an ongoing basis;

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

(5) consult with government agencies and standards development organizations as appropriate;

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

(7) 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

(8) 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) as appropriate, other organizations, other interested Federal, State, and local agencies, and other interested persons.

[(c)] *(e)* MISCELLANEOUS PROVISIONS.—

(1) * * *

* * * * * * *

SEC. 314. NATIONAL STANDARDS FOR HOMELAND SECURITY EQUIPMENT AND TRAINING.

(a) EQUIPMENT STANDARDS.—

(1) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, and in consultation with other components of the Department, as appropriate, and the National Institute of Standards and Technology, shall support the development, promulgation, and updating as necessary of national voluntary consensus standards for the performance, use, and validation of equipment used by Federal, State, and local government and nongovernment emergency response providers, and by the components of the Department. Such standards—

(A) shall be, to the maximum extent practicable, consistent with any existing voluntary consensus standards;

(B) shall take into account, as appropriate, new types of terrorism threats and responsibilities of the Department that may not have been contemplated when such existing standards were developed;

(C) shall be focused on maximizing interoperability, interchangeability, durability, flexibility, efficiency, efficacy, portability, sustainability, and safety; and

(D) shall cover all appropriate uses of the equipment.

(2) REQUIRED CATEGORIES.—In carrying out paragraph (1), the Secretary shall specifically consider national voluntary consensus standards for the performance, use, and validation of the following categories of equipment:

(A) Thermal imaging equipment.

(B) Radiation detection and analysis equipment.

(C) Biological detection and analysis equipment.

(D) Chemical detection and analysis equipment.

(E) Decontamination and sterilization equipment.

(F) Personal protective equipment, including garments, boots, gloves, and hoods and other protective clothing.

(G) Respiratory protection equipment.

(H) Interoperable communications, including wireless and wireline voice, video, and data networks.

(I) Explosive detection and analysis equipment, and technologies and methods to mitigate the impact of explosive devices or materials.

(J) Containment vessels.

(K) Contaminant-resistant vehicles.

(L) Aerial platforms.

(M) Special rescue equipment.

(N) Screening and patrolling technologies.

(O) Such other equipment for which the Secretary determines that national voluntary consensus standards would be appropriate.

(3) CERTIFICATION AND ACCREDITATION.—The Secretary, in carrying out this subsection, and in coordination with the Director of the National Institute of Standards and Technology,

may support the certification of equipment and the accreditation of laboratories to conduct testing and evaluation.

(4) EQUIPMENT STANDARDS AND ACQUISITIONS.—

(A) DEPARTMENT SUPPORTED ACQUISITIONS.—If an applicant for financial assistance provided by the Department proposes to use such financial assistance to upgrade or purchase new equipment or systems that do not meet or exceed any applicable national voluntary consensus standards, the applicant shall include in its application for financial assistance an explanation of why such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed such standards.

(B) DEPARTMENT ACQUISITIONS.—When an operational unit of the Department proposes to upgrade or purchase new equipment or systems, the head of that unit shall consult with the Under Secretary for Science and Technology on whether such equipment or systems meet or exceed any applicable national voluntary consensus standards and whether there is need for the Department to support the development or updating of applicable national voluntary consensus standards.

(b) TRAINING STANDARDS.—

(1) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, and in consultation with other components of the Department, as appropriate, shall support the development, promulgation, and regular updating as necessary of national voluntary consensus standards for training for Federal, State, and local government and nongovernment emergency response providers and Department personnel, including training that will enable them to use equipment effectively and appropriately in carrying out their responsibilities. Such standards shall give priority to providing training to—

(A) enable Federal, State, and local government and nongovernment emergency response providers and Department personnel to prevent, prepare for, respond to, mitigate against, and recover from terrorist threats, including threats from chemical, biological, radiological, and nuclear weapons and explosive devices capable of inflicting significant human casualties, and other emergencies; and

(B) familiarize Federal, State, and local government and nongovernment emergency response providers and Department personnel with the proper use of equipment, including software, developed pursuant to the standards developed under subsection (a).

(2) REQUIRED CATEGORIES.—In carrying out paragraph (1), the Secretary specifically shall include the following categories of activities:

(A) Regional planning.

(B) Joint exercises.

(C) Intelligence collection, analysis, and sharing.

(D) Decisionmaking protocols for incident response and alarms.

(E) Emergency notification of affected populations.

(F) Detection of biological, nuclear, radiological, and chemical weapons of mass destruction.

(G) Screening and patrolling procedures.

(H) Such other activities for which the Secretary determines that national voluntary consensus training standards would be appropriate.

(3) CONSISTENCY.—In carrying out this subsection, the Secretary shall ensure that—

(A) training standards for Federal, State, and local government and nongovernment emergency response providers are consistent with the principles of emergency preparedness for all hazards; and

(B) training standards for Department personnel are consistent with the counterterrorism and traditional responsibilities of the Department.

(c) CONSULTATION WITH STANDARDS ORGANIZATIONS.—In supporting the development, promulgation, and updating of national voluntary consensus standards for equipment for and training under this section, the Secretary shall consult with relevant public and private sector groups, including—

(1) the National Institute of Standards and Technology;

(2) the National Fire Protection Association;

(3) the National Association of County and City Health Officials;

(4) the Association of State and Territorial Health Officials;

(5) the American National Standards Institute;

(6) the National Institute of Justice;

(7) the Inter-Agency Board for Equipment Standardization and Interoperability;

(8) the National Public Health Performance Standards Program;

(9) the National Institute for Occupational Safety and Health;

(10) ASTM International;

(11) the International Safety Equipment Association;

(12) the Emergency Management Accreditation Program; and

(13) to the extent the Secretary considers appropriate, other national voluntary consensus standards development organizations, other interested Federal, State, and local agencies, and other interested persons.

(d) COORDINATION WITH SECRETARIES OF HHS AND TRANSPORTATION.—In supporting the development, promulgation, and updating of any national voluntary consensus standards under this section for equipment for or training of emergency response providers that involve or relate to health or emergency medical services professionals, including emergency medical professionals, the Secretary shall coordinate activities under this section with the Secretary of Health and Human Services and the Secretary of Transportation.

(e) CONSISTENCY WITH THE NATIONAL TECHNOLOGY TRANSFER AND ADVANCEMENT ACT.—In carrying out this section, the Secretary shall comply with section 12(d) of the National Technology Transfer and Advancement Act (15 U.S.C. 272 note).

SEC. 315. REGIONAL TECHNOLOGY INTEGRATION PROGRAM.

(a) IN GENERAL.—The Under Secretary for Science and Technology, in coordination with the Under Secretary for Preparedness, shall provide technical guidance, training, and other assistance, as appropriate, to support the transfer and integration of homeland security technologies and protocols in urban and other high risk juris-

dictions determined by the Secretary to be at consistently high levels of risk from terrorist attack.

(b) ACTIVITIES.—The program supported under subsection (a) shall work to—

(1) facilitate the transition of innovative technologies and operational concepts, including those described in subsection (c);

(2) integrate new technologies with existing infrastructure, systems, and concepts;

(3) identify capability and technology gaps for future research, development, test, and evaluation;

(4) evaluate system performance, life cycle, and human factor issues; and

(5) disseminate lessons learned to other communities.

(c) INNOVATIVE TECHNOLOGIES AND OPERATIONAL CONCEPTS.—The innovative technologies and operational concepts referred to in subsection (b)(1) include—

(1) detection systems for weapons of mass destruction;

(2) emergency management information systems;

(3) situational awareness;

(4) information sharing;

(5) atmospheric transport and dispersion modeling;

(6) public alerts and warnings;

(7) aerial platforms; and

(8) emergency medical support.

(d) COORDINATION.—In setting priorities for and carrying out the activities under this section, the Under Secretary for Science and Technology shall consult and coordinate with appropriate governors, mayors, other State and local government officials, and first responders.

SEC. 316. CYBERSECURITY RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—The Under Secretary for Science and Technology shall support research and development, including fundamental, long-term research, in cybersecurity to improve the ability of the United States to prevent, protect against, detect, respond to, and recover from cyber attacks, with emphasis on research and development relevant to large-scale, high-impact attacks.

(b) ACTIVITIES.—The research and development supported under subsection (a) shall include work to—

(1) advance the development and accelerate the deployment of more secure versions of critical information systems, including—

(A) fundamental Internet protocols and architectures, including for the domain name system and routing protocols; and

(B) control systems used in critical infrastructure sectors;

(2) improve and create technologies for detecting attacks or intrusions, including monitoring technologies;

(3) improve and create mitigation and recovery methodologies, including techniques for containment of attacks and development of resilient networks and systems that degrade gracefully; and

(4) develop and support infrastructure and tools to support cybersecurity research and development efforts, including mod-

eling, testbeds, and data sets for assessment of new cybersecurity technologies.

(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall coordinate activities with—

(1) the Assistant Secretary for Cybersecurity and Telecommunications; and

(2) other Federal agencies, including the National Science Foundation, the Defense Advanced Research Projects Agency, the Information Assurance Directorate of the National Security Agency, and the National Institute of Standards and Technology, to identify unmet needs and cooperatively support activities, as appropriate.

(d) NATURE OF RESEARCH.—Activities under this section shall be carried out in accordance with section 306(a) of this Act.

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section such sums as may be necessary for fiscal year 2007.

SEC. 317. STANDARDS FOR CRITICAL INFRASTRUCTURE INFORMATION SYSTEMS.

(a) STANDARDS PROGRAM.—The Under Secretary for Science and Technology shall establish a program to support the development and promulgation of national voluntary consensus standards for requirements, performance testing, and user training with respect to critical infrastructure information systems.

(b) PURPOSE.—The standards developed under subsection (a) shall be designed to assist State and local jurisdictions, including those in urban and other areas at consistently high levels of risk from terrorist attack, and emergency response providers to acquire and implement critical infrastructure information systems and to store and access information regarding critical infrastructure to be used in responding to acts of terrorism or other emergencies.

(c) REQUIREMENTS.—The standards developed under subsection (a) shall be designed to facilitate—

(1) the interoperability of systems to enable sharing of information in a variety of formats and across stakeholders at the Federal, State, and local levels;

(2) the ease of deployment of the systems to the field;

(3) the ability to retrieve situational awareness information in real-time;

(4) the integrity, security, and accessibility of stored information;

(5) the application of human factors science in the development of the system;

(6) the availability and content of training programs for potential users; and

(7) meeting any other requirements determined by the Under Secretary to be appropriate.

(d) REPORTS.—The Under Secretary for Science and Technology shall submit to Congress—

(1) 6 months after the date of enactment of this section, a report describing the plan for carrying out the program under this section, which shall include a schedule for the development of national voluntary consensus standards for critical infrastructure information systems; and

(2) 12 months after the date of enactment of this section, a report which shall include a description of—

(A) the steps taken under this program and the funding dedicated to this program; and

(B) the steps that have been or will be taken to promote the adoption of the standards by appropriate standard-setting organizations.

(e) DEFINITIONS.—In this section—

(1) the term "critical infrastructure information systems" means software programs that store, manage, and display information about critical infrastructure to support situational awareness and real-time decisionmaking of law enforcement, fire services, emergency medical services, emergency management agencies, other emergency response providers, and critical infrastructure facility stakeholders. Critical infrastructure information may include maps and other geospatial information, emergency plans, interior and exterior imagery, entry and exit points, and any other information about infrastructure or facilities that may be beneficial to users of critical infrastructure information systems; and

(2) the term "critical infrastructure" has the meaning given that term in section 1016(e) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (42 U.S.C. 5195c(e)).

SEC. 318. SCHOLARSHIP AND FELLOWSHIP PROGRAMS.

(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, shall encourage the development of an adequate supply of people trained in and performing research in science, technology, engineering, and mathematical fields relevant to homeland security.

(b) RESPONSIBILITIES.—In carrying out this section, the Secretary may support—

(1) programs at the undergraduate, graduate, and postdoctoral levels, including at Historically Black Colleges and Universities that are Part B institutions as defined in section 322(2) of the Higher Education Act of 1965 (20 U.S.C. 1061(2)) and minority institutions (as defined in section 365(3) of that Act (20 U.S.C. 1067k(3))); and

(2) internship programs that take advantage of the homeland security research infrastructure available to the Department, including laboratories owned or operated by the Department, the Department of Energy National Laboratories, and University Centers of Excellence.

SEC. 319. PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES ISSUES IN TECHNOLOGY DEVELOPMENT.

Not later than 180 days after the date of enactment of this section, the Under Secretary for Science and Technology, the Chief Privacy Officer, and the Officer for Civil Rights and Civil Liberties shall transmit to Congress a joint plan for how privacy and civil rights and civil liberties issues will be considered in technology research and development programs at the Department, including how such

issues will be taken into account in defining requirements for technology performance and use of technologies in pilot programs.

* * * * * * *

ADDITIONAL VIEWS

We welcome the unanimous passage of H.R. 4941, the "Homeland Security Science and Technology Enhancement Act of 2006," by the Committee on Homeland Security. The Department of Homeland Security's Science and Technology Directorate has experienced a rocky three years since it was created. The Directorate has lacked clear priorities and a long-term research and development strategy, despite the many talented hard-working career employees on staff. This legislation represents an important step in refocusing the Directorate and setting it on a path to success.

We are especially pleased with the provisions in this bill that will strengthen standards for first responder equipment and help with the transfer of technology from other sectors, such as the military, for use by firefighters, police, and paramedics.

Additionally, we are pleased that the Majority accepted the amendment offered by Rep. Nita Lowey (D–NY) to direct the Department's Under Secretary for Science and Technology to continue to work with the National Institute of Standards and Technology and other appropriate Federal agencies to assess the compliance of first responder communications equipment with the Project 25 standards established by the Association of Public Safety Communications Officials International (APCO). Project 25 is a set of standards for interoperable wireless communications systems. Any Project 25 radio should be able to work with any other Project 25 system. The Department should continue to work with the National Institute of Standards and Technology (NIST) to certify manufacturers' claims that communication equipment meets Project 25 standards so that when a public safety agency buys communication equipment, it is assured the standards are met and that the equipment will in fact be interoperable.

Ranking Member Thompson, Rep. Zoe Lofgren (D–CA), Rep. James Langevin (D–RI), and Rep. Sheila Jackson-Lee (D–TX) are pleased that the legislation includes their proposals to assist minority and disadvantaged populations to prepare for terrorist attacks and natural disasters. These provisions do the following:

• Require the Department to ensure minority-serving colleges and universities are represented in its scholarship and fellowship programs that promote education and research in science, technology, engineering, and mathematical fields relevant to homeland security. These institutions have a majority-minority population of students who can bring unique skills and backgrounds to the effort to secure the homeland.

• Require the Department to report to Congress on its use of social and behavioral research in its programs regarding emergency preparedness and response, search and rescue, evacuation, and sheltering in-place procedures for populations with special needs, including persons with disabilities, health problems, language bar-

riers, and income barriers, the elderly, and children. Hurricane Katrina demonstrated that the Department has difficulties communicating with special needs populations during emergencies. This provision will encourage the Department to better utilize social and behavioral research when reaching out to these communities.

We are also pleased that this bill lays out a detailed cyber security research and development agenda for the Department. Unfortunately, the bill only authorizes "such sums as may be necessary" for these activities in fiscal year 2007. We are disappointed the Committee rejected on a party-line vote Rep. Loretta Sanchez's (D–CA) amendment to provide $50 million for these activities in fiscal year 2007. We are concerned that a failure to authorize a specific amount for these activities will ensure the Department continues to fail to properly prioritize cyber security research and development. Moreover, we believe there are strong policy reasons to support the approximately $27 million increase in cyber security research and development that Ms. Sanchez's amendment would provide. This increase in funding could be used to improve cyber security research and development in three specific areas: (1) Cyber Situational Awareness and Cyber Security Operations Simulation and Modeling; (2) Emerging cyber security issues, including Identity Management, Voice Over IP security research, TCP/IP security, and Process Control Systems security; and (3) existing efforts, such as the national test bed for cyber security projects, the security of the Internet Domain Name System, and wireless security experiments. Without more research and development in these areas, our economy and entire nation will remain at risk from hackers, including terrorists. We note that Ms. Sanchez's amendment had strong support from much of the computer, Internet, and technology industries, as represented by the letters of support received from Internet Security Systems, the Cyber Security Alliance, and SRI International.

We note that during the debate on Rep. Sanchez's amendment, Rep. Curt Weldon (R–PA) expressed concerns about the amendment because he felt that the Department of Defense was already expending large sums of funding on cyber security research and development. According to industry sources, however, the Department of Defense's cyber research is not aimed at homeland security issues, such as securing the Internet, protecting domestic critical infrastructure, strengthening first responder systems, or combating fraud. Instead, its research is focused on developing new communications technologies to support forward deployed forces and protect defense information systems. Indeed, the Department of Defense's research is actually focused on developing well-separated networks to reduce the military's dependence on the Internet. Additionally, the Department of Defense is not investing in high-risk research and development to create commercially viable defenses against the multi-billion dollar transnational threat of organized crime behind the waves of phishing, crime-ware, and identity theft already impacting millions of Americans. Department of Homeland Security research, on the other hand, focuses on the Internet and threats to other critical infrastructure that are key parts of our national economy or threaten large numbers of people's lives. We

hope that Members understand the fundamental differences between the two agencies.

We are also disappointed that the Committee accepted on a party-line vote a second degree amendment by Rep. Christopher Shays (R–CT) to strike $150 million in funding for rail and mass transit security research and development over three years provided in an amendment offered by Rep. Eleanor Holmes Norton (D–DC).

The threat terrorists pose to rail and mass transit in the United States is genuine, as demonstrated by the thousands killed or injured in attacks in London, Madrid, Moscow, Tokyo and elsewhere in the last decade. Indeed, terrorists have already carried out attacks on rail systems in the United States. In 1995, domestic terrorists calling themselves "Sons of Gestapo" pulled 29 spikes from a stretch of railroad track in the Arizona desert, sending an Amtrak train off a bridge, resulting in the death of one person and the injury of 78 people.

We recognize that the open and rapid nature of rail and mass transit makes it more difficult to secure than other modes of transportation, such as aviation, but we believe that improved technology can help to close this security gap. Unfortunately, the Department of Homeland Security has conducted little substantial research and development in this area. If accepted in its entirety, Rep. Norton's amendment would have focused $150 million over three years on reducing the vulnerability of passenger trains, stations, and equipment; transportation of hazardous material by rail; bridges and tunnels; and other key areas of rail security research. As a result of the passage of Rep. Shay's second degree amendment, there will be no guaranteed funding for these activities.

CONCLUSION

While we support the underlying provisions in H.R. 4941, and appreciate the bipartisan way in which this bill was developed, we regret that the Majority was unwilling to make commitments to provide a specific amount of funding for cyber security and rail and mass transit research and development. Without providing a specific amount of funding for these activities, we do not believe that the Department will focus enough on these efforts. As a result, our nation's economy will remain at risk especially its Internet, technology, and computer industry—and thousands of passengers will not be adequately protected from attacks on the rail or mass transit systems they use every day.

BENNIE G. THOMPSON.
ZOE LOFGREN.
BOB ETHERIDGE.
KENDRICK B. MEEK.
LORETTA SANCHEZ.
BILL PASCRELL, Jr.
JAMES R. LANGEVIN.
ED MARKEY.
JANE HARMAN.
NITA M. LOWEY.
DONNA M. CHRISTENSEN.

NORMAN DICKS.
PETER DE FAZIO.
SHEILA JACKSON-LEE.
ELEANOR HOLMES NORTON.

○