AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

109TH CONGRESS, 2d Session | HOUSE OF REPRESENTATIVES | REPT. 109–447, Part 1

SECURITY AND ACCOUNTABILITY FOR EVERY PORT ACT

APRIL 28, 2006.—Ordered to be printed

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

R E P O R T

together with

MINORITY, DISSENTING, AND ADDITIONAL VIEWS

[To accompany H.R. 4954]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 4954) to improve maritime and cargo security through enhanced layered defenses, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
Purpose and Summary	33
Background and Need for Legislation	33
Hearings and Briefings	34
Committee Consideration	37
Committee Votes	37
Committee Oversight Findings	65
Statement of General Performance Goals and Objectives	65
New Budget Authority, Entitlement Authority, and Tax Expenditures	65
Congressional Budget Office Estimate	65
Federal Mandates Statement	70
Advisory Committee Statement	70
Constitutional Authority Statement	70
Applicability to Legislative Branch	70
Section-by-Section Analysis of the Legislation	70
Changes in Existing Law Made by the Bill, as Reported	99
Minority and Dissenting Views	143
Letters and Correspondence	150

The amendment is as follows:

49–006

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Security and Accountability For Every Port Act" or "SAFE Port Act".

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

Sec. 1. Short title; table of contents.
Sec. 2. Findings.
Sec. 3. Definitions.

TITLE I—SECURITY OF UNITED STATES SEAPORTS

Subtitle A—General Provisions

Sec. 101. Definition of transportation security incident.
Sec. 102. Protocols for resumption of trade.
Sec. 103. Requirements relating to maritime facility security plans.
Sec. 104. Unannounced inspections of maritime facilities.
Sec. 105. Verification of individuals with access to secure areas of seaports.
Sec. 106. Clarification on eligibility for transportation security cards.
Sec. 107. Long-range vessel tracking.
Sec. 108. Maritime security command centers.

Subtitle B—Grant and Training Programs

Sec. 111. Port security grant program.
Sec. 112. Port security training program.
Sec. 113. Port security exercise program.
Sec. 114. Reserve officers and junior reserve officers training pilot project.

Subtitle C—Miscellaneous Provisions

Sec. 121. Increase in port of entry inspection officers.
Sec. 122. Acceleration of Integrated Deepwater System.
Sec. 123. Border Patrol unit for United States Virgin Islands.
Sec. 124. Report on ownership and operation of United States seaports.
Sec. 125. Report on security operations at certain United States seaports.
Sec. 126. Report on arrival and departure manifests for certain commercial vessels in the United States Virgin Islands.

TITLE II—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN

Sec. 201. Security of the international supply chain.
Sec. 202. Next generation supply chain security technologies.
Sec. 203. Uniform data system for import and export information.
Sec. 204. Foreign port assessments.
Sec. 205. Pilot program to improve the security of empty containers.
Sec. 206. Study and report on advanced imagery pilot programs.

TITLE III—DIRECTORATE FOR POLICY, PLANNING, AND INTERNATIONAL AFFAIRS

Sec. 301. Establishment of Directorate.

TITLE IV—OFFICE OF DOMESTIC NUCLEAR DETECTION

Sec. 401. Establishment of Office.
Sec. 402. Nuclear and radiological detection systems.

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) Maritime vessels are the primary mode of transportation for international trade and they carry over 80 percent of international trade by volume.

(2) In 2004, maritime vessels carried approximately 9,700,000 shipping containers into United States seaports at an average of 27,000 containers per day.

(3) The security of the international container supply chain and the maritime transportation system is critical for the prosperity and liberty of all countries.

(4) In its final report, the National Commission on Terrorist Attacks Upon the United States noted, "While commercial aviation remains a possible target, terrorists may turn their attention to other modes of transportation. Opportunities to do harm are as great, or greater in maritime or surface transportation.".

(5) In May 2002, the Brookings Institution estimated that costs associated with United States port closures from a detonated terrorist weapon could add up to $1 trillion from the resulting economic slump and changes in our Nation's inability to trade. Anticipated port closures on the west coast of the United States could cost the United States economy $1 billion per day for the first five days after a terrorist attack.

(6) Significant steps have been taken since the terrorist attacks against the United States that occurred on September 11, 2001:

(A) Congress passed the Maritime Transportation Security Act of 2002 on November 14, 2002.

(B) The Coast Guard issued a comprehensive set of port security regulations on October 22, 2003.

(C) The International Maritime Organization adopted the International Ship and Port Facility (ISPS) Code in December 2002.

(D) The White House issued Homeland Security Presidential Directive-13 in September 2005 which lays out requirements for a comprehensive maritime security policy.

(7) Through both public and private projects, the private sector in the United States and overseas has worked with the Department of Homeland Security to improve the security of the movement of cargo through the international supply chain.

(8) Despite these steps, security gaps in the maritime transportation system remain, resulting in high-risk container systems not being checked overseas or domestically and ports that are vulnerable to terrorist attacks similar to the attack on the U.S.S. Cole.

(9) Significant enhancements can be achieved by applying a multi-layered approach to supply chain security, in a coordinated fashion. Current supply chain programs within the Federal Government have been independently operated, often falling short of gains which could have been made if such programs were operated in a coordinated manner with clear system standards and a framework that creates incentives for security investments.

(10) While it is impossible to completely remove the risk of a terrorist attack, security measures in the supply chain can add certainty and stability to the global economy, raise investor confidence, and facilitate trade. Some counterterrorism costs are integral to the price that must be paid to protect society. However, counterterrorism measures also present an opportunity to increase the efficiency of the global trade system through international harmonization of such measures. These efficiency gains are maximized when all countries adopt such counterterrorism measures.

(11) Increasing transparency in the supply chain will assist in mitigating the impact of a terrorist attack by allowing for a targeted shutdown of the international supply chain and expedited restoration of commercial traffic.

SEC. 3. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" has the meaning given the term in section 2(2) of the Homeland Security Act of 2002 (6 U.S.C. 101(2)).

(2) DEPARTMENT.—The term "Department" means the Department of Homeland Security.

(3) INTERNATIONAL SUPPLY CHAIN.—The term "international supply chain" means the end-to-end process for shipping goods from a point of origin overseas to and from the United States.

(4) SECRETARY.—The term "Secretary" means the Secretary of Homeland Security.

TITLE I—SECURITY OF UNITED STATES SEAPORTS

Subtitle A—General Provisions

SEC. 101. DEFINITION OF TRANSPORTATION SECURITY INCIDENT.

Section 70101(6) of title 46, United States Code, is amended by inserting after "economic disruption" the following "(other than economic disruption caused by acts that are unrelated to terrorism and are committed during a labor strike, demonstration, or other type of labor unrest)".

SEC. 102. PROTOCOLS FOR RESUMPTION OF TRADE.

(a) IN GENERAL.—Section 70103(a)(2)(J) of title 46, United States Code, is amended—

(1) by striking "(J)" and inserting "(J)(i)"; and

(2) by adding at the end the following new clause:

"(ii) The plan required by clause (i) shall include protocols for the resumption of trade in the event of a transportation security incident that necessitates the suspension of trade through contingency and continuity planning that ensures trade lanes are restored as quickly as possible. The protocols shall provide for—

"(I) coordination with appropriate Federal, State, and local agencies, the private sector, and appropriate overseas entities in developing such contingency and continuity planning;

"(II) coordination with appropriate Federal, State, and local agencies and the private sector on law enforcement actions, inter-modal rerouting plans, and identification and prioritization of goods that may enter the United States; and

"(III) designation of appropriate Federal officials to work with port authorities to reestablish the flow of cargo by prioritizing shipments based on appropriate factors, including factors relating to public health, national security, and economic need.".

(b) EFFECTIVE DATE.—The Secretary of Homeland Security shall develop the protocols described in section 70103(a)(2)(J)(ii) of title 46, United States Code, as added by subsection (a), not later than 180 days after the date of the enactment of this Act.

SEC. 103. REQUIREMENTS RELATING TO MARITIME FACILITY SECURITY PLANS.

(a) FACILITY SECURITY PLANS.—The Secretary of Homeland Security shall require that a security plan for a facility required under section 70103(c) of title 46, United States Code, shall be resubmitted for approval upon transfer of ownership or operation of such facility.

(b) FACILITY SECURITY OFFICERS.—

(1) IN GENERAL.—The Secretary shall require that the qualified individual having full authority to implement security actions who is required to be identified under section 70103(c)(3)(B) of title 46, United States Code, for a facility described in section 70103(c)(2) of that title shall be a citizen of the United States.

(2) WAIVER.—The Secretary may waive the requirement of paragraph (1) with respect to an individual if the Secretary determines that it is appropriate to do so based on a complete background check of the individual and a review of all terrorist watchlists to ensure that the individual is not identified on any such terrorist watchlist.

(c) FACILITY SECURITY ACCESS.—Section 70103(c)(3)(C)(ii) of title 46, United States Code, is amended by adding at the end before the semicolon the following: ", including access by individuals engaged in the surface transportation of intermodal containers in or out of a port facility".

SEC. 104. UNANNOUNCED INSPECTIONS OF MARITIME FACILITIES.

Subparagraph (D) of section 70103(c)(4) of title 46, United States Code, is amended to read as follows:

"(D) verify the effectiveness of each such facility security plan periodically, but not less than twice annually, at least one of which shall be an inspection of the facility that is conducted without notice to the facility.".

SEC. 105. VERIFICATION OF INDIVIDUALS WITH ACCESS TO SECURE AREAS OF SEAPORTS.

(a) IMPLEMENTATION OF REQUIREMENTS.—Notwithstanding any other provision of law, the Secretary of Homeland Security shall—

(1) not later than July 15, 2006, issue a notice of proposed rulemaking for regulations required to implement section 70105 of title 46, United States Code;

(2) not later than November 15, 2006, issue final regulations required to implement that section; and

(3) begin issuing transportation security cards to individuals at seaports facilities under subsection (b) of that section in accordance with the schedule contained in subsection (b)(2) of this section.

(b) TRANSPORTATION SECURITY CARDS.—

(1) MANAGEMENT.—Final regulations issued under subsection (a)(2) shall provide for Federal management of the system for issuing transportation security cards.

(2) SCHEDULE FOR ISSUING TRANSPORTATION SECURITY CARDS AT SEAPORTS.—

(A) Not later than May 15, 2007, the Secretary shall begin issuing transportation security cards to individuals at the first 25 seaport facilities listed on the facility vulnerability assessment issued by the Secretary under section 70102 of title 46, United States Code.

(B) Not later than November 15, 2007, the Secretary shall begin issuing transportation security cards to individuals at the next 30 seaport facilities listed on that assessment.

(C) Not later than November 15, 2008, the Secretary shall issue transportation security cards to individuals at all other seaport facilities.

(c) INTERIM VERIFICATION OF INDIVIDUALS.—

(1) TERRORIST WATCH LIST COMPARISON AND IMMIGRATION RECORDS CHECK.—Not later than 90 days after the date of enactment of this Act, the Secretary shall—

(A) complete a comparison of each individual who has unescorted access to a secure area of a seaport facility (as designated in an approved facility security plan in accordance with section 70103(c) of title 46, United States Code) against terrorist watch lists to determine if the individual poses a threat; and

(B) determine whether each such individual may be denied admission to the United States, or removed from the United States, under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(2) CONTINUING REQUIREMENT.—In the case of an individual who is given unescorted access to a secure area of a seaport facility after the date on which the Secretary completes the requirements of paragraph (1) and before the date on which the Secretary begins issuing transportation security cards at the seaport facility, the Secretary shall conduct a comparison of the individual against terrorist watch lists and determine whether the individual is lawfully present in the United States.

(3) INTERIM FINAL REGULATIONS.—In order to carry out this subsection, the Secretary shall issue interim final regulations to require submission to the Secretary of information necessary to carry out the requirements of paragraph (1).

(4) PRIVACY REQUIREMENTS.—Terrorist watch list comparisons and immigration records checks under this subsection shall be carried out in accordance with the requirements of section 552a of title 5, United States Code.

(5) RESTRICTIONS ON USE AND MAINTENANCE OF INFORMATION.—

(A) RESTRICTION ON DISCLOSURE.—Information obtained by the Secretary in the course of comparing the individual against terrorist watch lists under this subsection may not be made available to the public, including the individual's employer.

(B) CONFIDENTIALITY; USE.—Any information constituting grounds for prohibiting the employment of an individual in a position described in paragraph (1)(A) shall be maintained confidentially by the Secretary and may be used only for making determinations under this section. The Secretary may share any such information with appropriate Federal, State, local, and tribal law enforcement agencies.

(6) TERRORIST WATCH LISTS DEFINED.—In this subsection, the term "terrorist watch lists" means all available information on known or suspected terrorists or terrorist threats.

(d) REPORTING.—Not later than 120 days after the date of enactment of this Act, the Secretary shall submit to the appropriate congressional committees a report containing information on—

(1) the number of matches made in conducting terrorist watch list comparisons, and the number of individuals found to be unlawfully present in the United States, under subsection (c);

(2) the corresponding seaport facilities at which the matches and unlawfully present individuals were identified; and

(3) the actions taken as a result of the terrorist watchlist comparisons and immigration records checks under subsection (c).

(e) TREATMENT OF INDIVIDUALS RECEIVING HAZARDOUS MATERIALS ENDORSEMENTS.—

(1) IN GENERAL.—To the extent the Secretary determines that the background records check conducted under section 5103a of title 49, United States Code, and the background records check conducted under section 70105 of title 46, United States Code, are equivalent, the Secretary shall determine that an individual does not pose a risk warranting denial of a transportation security card issued under section 70105 of title 46, United States Code, if such individual—

(A) has successfully completed a background records check under section 5103a of title 49, United States Code; and

(B) possesses a current and valid hazardous materials endorsement in accordance with section 1572 of title 49, Code of Federal Regulations.

(2) LIMITATIONS.—Notwithstanding paragraph (1), the Secretary may deny an individual a transportation security card under section 70105 of title 46, United States Code, if the Secretary has substantial evidence that the individual poses a risk to national security.

(3) REDUCTION IN FEES.—The Secretary shall reduce, to the extent practicable, any fees associated with obtaining a transportation security card under section 70105 of title 46, United States Code, for any individual referred to in paragraph (1).

(f) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $20,000,000 for fiscal year 2007 to carry out this section.

SEC. 106. CLARIFICATION ON ELIGIBILITY FOR TRANSPORTATION SECURITY CARDS.

Section 70105(c)(2) of title 46, United States Code, is amended by inserting "subparagraph (A), (B), or (D) of" before "paragraph (1)".

SEC. 107. LONG-RANGE VESSEL TRACKING.

(a) REGULATIONS.—Section 70115 of title 46, United States Code is amended in the first sentence by striking "The Secretary" and inserting "Not later than April 1, 2007, the Secretary".

(b) VOLUNTARY PROGRAM.—The Secretary of Homeland Security may issue regulations to establish a voluntary long-range automated vessel tracking system for vessels described in section 70115 of title 46, United States Code, during the period before regulations are issued under subsection (a) of such section.

SEC. 108. MARITIME SECURITY COMMAND CENTERS.

(a) IN GENERAL.—Chapter 701 of title 46, United States Code, is amended by adding at the end the following new section:

"§ 70122. Maritime security command centers

"(a) ESTABLISHMENT.—The Secretary shall establish an integrated network of virtual and physical maritime security command centers at appropriate United States seaports and maritime regions, as determined by the Secretary, to—

"(1) enhance information sharing;

"(2) facilitate day-to-day operational coordination; and

"(3) in the case of a transportation security incident, facilitate incident management and response.

"(b) CHARACTERISTICS.—Each maritime security command center described in subsection (a) shall—

"(1) be regionally based and utilize where available the compositional and operational characteristics, facilities and information technology systems of current operational centers for port and maritime security and other similar existing facilities and systems;

"(2) be adapted to meet the security needs, requirements, and resources of the seaport and maritime region the center will cover; and

"(3) to the maximum extent practicable, not involve the construction of new facilities, but shall utilize information technology, virtual connectivity, and existing facilities to create an integrated, real-time communication and information sharing network.

"(c) PARTICIPATION.—The following entities shall participate in the integrated network of maritime security command centers described in subsection (a):

"(1) The Coast Guard.

"(2) U.S. Customs and Border Protection.

"(3) U.S. Immigration and Customs Enforcement.

"(4) Other appropriate Federal, State, and local law enforcement agencies.

"(d) RESPONSIBILITIES.—Each maritime security command center described in subsection (a) shall—

"(1) assist, as appropriate, in the implementation of maritime transportation security plans developed under section 70103;

"(2) implement the transportation security incident response plans required under section 70104;

"(3) carry out information sharing activities consistent with those activities required under section 1016 of the National Security Intelligence Reform Act of 2004 (6 U.S.C. 485) and the Homeland Security Information Sharing Act (6 U.S.C. 481 et seq.);

"(4) conduct short- and long-range vessel tracking under sections 70114 and 70115; and

"(5) carry out such other responsibilities as determined by the Secretary.

"(e) SECURITY CLEARANCES.—The Secretary shall sponsor and expedite individuals participating in a maritime security command center described in subsection (a) in gaining or maintaining their security clearances. Through the Captain of the Port, the Secretary may identify key individuals who should participate. In addition, the port or other entities may appeal to the Captain of the Port for sponsorship.

"(f) SECURITY INCIDENTS.—During a transportation security incident involving the port, the Coast Guard Captain of the Port designated by the Commandant of the Coast Guard in a maritime security command center described in subsection (a) shall act as the incident commander, unless otherwise directed by the President.

"(g) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to affect the normal command and control procedures for operational entities in the Department, unless so directed by the Secretary.

"(h) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated $60,000,000 for each of the fiscal years 2007 through 2012 to carry out this section and section 108(c) of the Security and Accountability For Every Port Act.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 701 of title 46, United States Code, is amended by adding at the end the following:

"70122. Maritime security command centers.".

(c) IMPLEMENTATION PLAN AND BUDGET ANALYSIS.—The Secretary of Homeland Security shall submit to the appropriate congressional committees a plan for the implementation of section 70122 of title 46, United States Code, as added by subsection (a), and a budget analysis for the implementation of such section, including additional cost-sharing arrangements with other Federal departments and agencies and other participants involved in the maritime security command centers described in such section, not later than 180 days after the date of the enactment of this Act.

Subtitle B—Grant and Training Programs

SEC. 111. PORT SECURITY GRANT PROGRAM.

(a) IN GENERAL.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.) is amended—

(1) by redesignating the second section 510 (as added by section 7303(d) of Public Law 108–458 (118 Stat. 3844)) as section 511; and

(2) by adding at the end the following new section:

"SEC. 512. PORT SECURITY GRANT PROGRAM.

"(a) GRANTS AUTHORIZED.—The Secretary shall establish a grant program to allocate Federal financial assistance to United States seaports on the basis of risk and need.

"(b) PRIORITIZATION PROCESS.—In awarding grants under this section, the Secretary shall conduct an assessment of United States seaports to develop a prioritization for awarding grants authorized under subsection (a) based upon—

"(1) the most current risk assessment available from the Department;

"(2) the national economic and strategic defense considerations of individual ports; and

"(3) any other factors that the Secretary determines to be appropriate.

"(c) APPLICATION.—

"(1) IN GENERAL.—Any entity or facility subject to an Area Maritime Transportation Security Plan required under subsection (b) or (c) of section 70103 of title 46, United States Code, may submit an application for a grant under this section, at such time, in such form, and containing such information and assurances as the Secretary may require.

"(2) MINIMUM STANDARDS FOR PAYMENT OR REIMBURSEMENT.—Each application submitted under paragraph (1) shall include—

"(A) a comprehensive description of—

"(i) the purpose of the project for which the applicant seeks a grant under this section and why the applicant needs the grant;

"(ii) the applicability of the project to the Area Maritime Transportation Security Plan and other homeland security plans;

"(iii) the methodology for coordinating the project into the security of the greater port area, as identified in the Area Maritime Transportation Security Plan;

"(iv) any existing cooperation or mutual aid agreements with other port facilities, vessels, organizations, or State, territorial, and local governments as such agreements relate to port security; and

"(v) a capital budget showing how the applicant intends to allocate and expend the grant funds;

"(B) a determination by the Captain of the Port that the project—

"(i) addresses or corrects port security vulnerabilities; and

"(ii) helps to ensure compliance with the Area Maritime Transportation Security Plan.

"(3) PROCEDURAL SAFEGUARDS.—The Secretary, in consultation with the Office of the Inspector General and the Office of Grants and Training, shall issue guidelines to establish appropriate accounting, reporting, and review procedures to ensure that—

"(A) grant funds are used for the purposes for which they were made available;

"(B) grantees have properly accounted for all expenditures of grant funds; and

"(C) grant funds not used for such purposes and amounts not obligated or expended are returned.

"(d) USE OF FUNDS.—Grants awarded under this section may be used—

"(1) to help implement Area Maritime Transportation Security Plans required under section 70103(b) of title 46, United States Code;

"(2) to remedy port security vulnerabilities identified through vulnerability assessments approved by the Secretary;

"(3) for non-Federal projects contributing to the overall security of a seaport or a system of United States seaports, as determined by the Secretary;

"(4) for the salaries, benefits, overtime compensation, and other costs of additional security personnel for State and local agencies for activities required by the Area Maritime Transportation Security Plan for a seaport area if the Secretary—

"(A) increases the threat level under the Homeland Security Advisory System to Code Orange or Code Red; or

"(B) raises the Maritime Security level to MARSEC Level 2 or 3;

"(5) for the cost of acquisition, operation, and maintenance of equipment that contributes to the overall security of the port area, as identified in the Area Maritime Transportation Security Plan, if the need is based upon vulnerability assessments approved by the Secretary or identified in the Area Maritime Security Plan;

"(6) to conduct vulnerability assessments approved by the Secretary;

"(7) to purchase or upgrade equipment, including computer software, to enhance terrorism preparedness;

"(8) to conduct exercises or training for prevention and detection of, preparedness for, response to, or recovery from terrorist attacks;

"(9) to establish or enhance mechanisms for sharing terrorism threat information;

"(10) for the cost of equipment (including software) required to receive, transmit, handle, and store classified information;

"(11) for the protection of critical infrastructure against potential attack by the addition of barriers, fences, gates, and other such devices, except that the cost of such measures may not exceed the greater of—

"(A) $1,000,000 per project; or

"(B) such greater amount as may be approved by the Secretary, which may not exceed 10 percent of the total amount of the grant; and

"(12) to conduct port-wide exercises to strengthen emergency preparedness of Federal, State, territorial, and local officials responsible for port security, including law enforcement personnel and firefighters and other first responders, in support of the Area Maritime Security Plan.

"(e) PROHIBITED USES.—Grants awarded under this section may not be used to—

"(1) supplant State or local funds for activities of the type described in subsection (d);

"(2) construct buildings or other physical facilities;

"(3) acquire land; or

"(4) make any State or local government cost-sharing contribution.

"(f) MATCHING REQUIREMENT.—

"(1) IN GENERAL.—Except as provided in subparagraph (A) or (B) of paragraph (2), Federal funds for any eligible project under this section shall not exceed 75 percent of the total cost of such project.

"(2) EXCEPTIONS.—

"(A) SMALL PROJECTS.—The requirement of paragraph (1) shall not apply with respect to a project with a total cost of not more than $25,000.

"(B) HIGHER LEVEL OF FEDERAL SUPPORT REQUIRED.—The requirement of paragraph (1) shall not apply with respect to a project if the Secretary determines that the project merits support and cannot be undertaken without a higher rate of Federal support than the rate described in paragraph (1).

"(3) IN-KIND CONTRIBUTIONS.—Each recipient of a grant under this section may meet the requirement of paragraph (1) by making in-kind contributions of goods or services that are directly linked with the purpose for which the grant is made, as determined by the Secretary, including any necessary personnel expenses, contractor services, administrative costs, equipment, fuel, or maintenance, and rental space.

"(g) MULTIPLE PHASE PROJECTS.—

"(1) IN GENERAL.—The Secretary may award grants under this section for projects that span multiple years.

"(2) FUNDING LIMITATION.—Not more than 20 percent of the total grant funds awarded under this section in any fiscal year may be awarded for projects that span multiple years.

"(h) CONSISTENCY WITH PLANS.—The Secretary shall ensure that each grant awarded under this section—

"(1) is used to supplement and support, in a consistent and coordinated manner, the applicable Area Maritime Transportation Security Plan; and

"(2) is coordinated with any applicable State or Urban Area Homeland Security Plan.

"(i) COORDINATION AND COOPERATION.—The Secretary—

"(1) shall ensure that all projects that receive grant funding under this section within any area defined in an Area Maritime Transportation Security Plan are coordinated with other projects in such area; and

"(2) may require cooperative agreements among users of the seaport and seaport facilities with respect to projects funded under this section.

"(j) REVIEW AND AUDITS.—The Secretary shall require all grantees under this section to maintain such records as the Secretary may require and make such records available for review and audit by the Secretary, the Comptroller General of the United States, or the Inspector General of the Department.

"(k) AUTHORIZATION OF APPROPRIATIONS.—

"(1) IN GENERAL.—There are authorized to be appropriated $400,000,000 for each of fiscal years 2007 through 2012 to carry out this section.

"(2) SOURCE OF FUNDS.—Amounts authorized to be appropriated under paragraph (1) shall originate from duties collected by U.S. Customs and Border Protection.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (116 Stat. 2135) is amended by inserting after the item relating to section 509 the following:

"Sec. 510. Procurement of security countermeasures for strategic national stockpile.
"Sec. 511. Urban and other high risk area communications capabilities.
"Sec. 512. Port security grant program.".

(c) REPEAL.—

(1) IN GENERAL.—Section 70107 of title 46, United States Code, is hereby repealed.

(2) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 701 of title 46, United States Code, is amended by striking the item relating to section 70107.

SEC. 112. PORT SECURITY TRAINING PROGRAM.

(a) IN GENERAL.—Subtitle A of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 361) is amended by adding at the end the following new section:

"SEC. 802. PORT SECURITY TRAINING PROGRAM.

"(a) IN GENERAL.—The Secretary, acting through the Assistant Secretary for Grants and Training and in coordination with components of the Department with maritime security expertise, including the Coast Guard, the Transportation Security Administration, and U.S. Customs and Border Protection, shall establish a Port Security Training Program (hereinafter in this section referred to as the 'Program') for the purpose of enhancing the capabilities of each of the Nation's commercial seaports to prevent, prepare for, respond to, mitigate against, and recover from threatened or actual acts of terrorism, natural disasters, and other emergencies.

"(b) REQUIREMENTS.—The Program shall provide validated training that—

"(1) reaches multiple disciplines, including Federal, State, and local government officials, commercial seaport personnel and management, and governmental and nongovernmental emergency response providers;

"(2) provides training at the awareness, performance, and management and planning levels;

"(3) utilizes multiple training mediums and methods, including—

"(A) direct delivery;

"(B) train-the-trainer;

"(C) computer-based training;

"(D) web-based training; and

"(E) video teleconferencing;

"(4) addresses port security topics, including—

"(A) seaport security plans and procedures, including how security plans and procedures are adjusted when threat levels increase;

"(B) seaport security force operations and management;

"(C) physical security and access control at seaports;

"(D) methods of security for preventing and countering cargo theft;

"(E) container security;

"(F) recognition and detection of weapons, dangerous substances, and devices;

"(G) operation and maintenance of security equipment and systems;

"(H) security threats and patterns;

"(I) security incident procedures, including procedures for communicating with governmental and nongovernmental emergency response providers; and

"(J) evacuation procedures;

"(5) is consistent with, and supports implementation of, the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goal, and other such national initiatives;

"(6) is evaluated against clear and consistent performance measures; and

"(7) addresses security requirements under facility security plans.

"(c) NATIONAL VOLUNTARY CONSENSUS STANDARDS.—The Secretary shall—

"(1) support the development, promulgation, and regular updating as necessary of national voluntary consensus standards for port security training; and

"(2) ensure that the training provided under this section is consistent with such standards.

"(d) TRAINING PARTNERS.—In developing and delivering training under the Program, the Secretary shall—

"(1) work with government training facilities, academic institutions, private organizations, employee organizations, and other entities that provide specialized, state-of-the-art training for governmental and nongovernmental emergency responder providers or commercial seaport personnel and management; and

"(2) utilize, as appropriate, training courses provided by community colleges, public safety academies, State and private universities, and other facilities.

"(e) CONSULTATION.—The Secretary shall ensure that, in carrying out the Program, the Office of Grants and Training shall consult with—

"(1) a geographic and substantive cross section of governmental and nongovernmental emergency response providers; and

"(2) commercial seaport personnel and management.

"(f) COMMERCIAL SEAPORT PERSONNEL DEFINED.—For purposes of this section, the term 'commercial seaport personnel' means any person engaged in an activity relating to the loading or unloading of cargo, the movement or tracking of cargo, the maintenance and repair of intermodal equipment, the operation of cargo-related equipment (whether or not integral to the vessel), and the handling of mooring lines on the dock when a vessel is made fast or let go, in the United States or the coastal waters thereof.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (116 Stat. 2135) is amended by inserting after the item relating to section 801 the following:

"Sec. 802. Port security training program.".

(c) VESSEL AND FACILITY SECURITY PLANS.—Section 70103(c)(3) of title 46, United States Code, is amended—

(1) in subparagraph (E), by striking "the training, periodic unannounced drills, and"

(2) by redesignating subparagraphs (F) and (G) as subparagraphs (G) and (H), respectively; and

(3) by inserting after subparagraph (E) the following new subparagraph:

"(F) provide a strategy and timeline for conducting training and periodic unannounced drills for persons on the vessel or at the facility to be carried out under the plan to deter, to the maximum extent practicable, a transportation security incident or a substantial threat of such a transportation security incident;".

SEC. 113. PORT SECURITY EXERCISE PROGRAM.

(a) IN GENERAL.—Subtitle A of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 361), as amended by section 112, is further amended by adding at the end the following new section:

"SEC. 803. PORT SECURITY EXERCISE PROGRAM.

"(a) IN GENERAL.—The Secretary, acting through the Assistant Secretary for Grants and Training, shall establish a Port Security Exercise Program (hereinafter in this section referred to as the 'Program') for the purpose of testing and evaluating the capabilities of Federal, State, local, and foreign governments, commercial seaport personnel and management, governmental and nongovernmental emergency response providers, the private sector, or any other organization or entity, as the Secretary determines to be appropriate, to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism, natural disasters, and other emergencies at commercial seaports.

"(b) REQUIREMENTS.—The Secretary, acting through the Assistant Secretary for Grants and Training and in coordination with components of the Department with

maritime security expertise, including the Coast Guard, the Transportation Security Administration, and U.S. Customs and Border Protection, shall ensure that the Program—

"(1) consolidates all existing port security exercise programs administered by the Department;

"(2) conducts, on a periodic basis, port security exercises at commercial seaports that are—

"(A) scaled and tailored to the needs of each port;

"(B) live in the case of the most at-risk ports;

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

"(D) consistent with the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goal, and other such national initiatives;

"(E) evaluated against clear and consistent performance measures;

"(F) assessed to learn best practices, which shall be shared with appropriate Federal, State, and local officials, seaport personnel and management; governmental and nongovernmental emergency response providers, and the private sector; and

"(G) followed by remedial action in response to lessons learned; and

"(3) assists State and local governments and commercial seaports in designing, implementing, and evaluating exercises that—

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

"(B) are consistent with any applicable Area Maritime Transportation Security Plan and State or Urban Area Homeland Security Plan.

"(c) REMEDIAL ACTION MANAGEMENT SYSTEM.—The Secretary, acting through the Assistant Secretary for Grants and Training, shall establish a Remedial Action Management System to—

"(1) identify and analyze each port security exercise for lessons learned and best practices;

"(2) disseminate lessons learned and best practices to participants in the Program;

"(3) monitor the implementation of lessons learned and best practices by participants in the Program; and

"(4) conduct remedial action tracking and long-term trend analysis.

"(d) GRANT PROGRAM FACTOR.—In evaluating and prioritizing applications for Federal financial assistance under section 512, the Secretary shall give additional consideration to those applicants that have conducted port security exercises under this section.

"(e) CONSULTATION.—The Secretary shall ensure that, in carrying out the Program, the Office of Grants and Training shall consult with—

"(1) a geographic and substantive cross section of governmental and nongovernmental emergency response providers; and

"(2) commercial seaport personnel and management.

"(f) COMMERCIAL SEAPORT PERSONNEL DEFINED.—For purposes of this section, the term 'commercial seaport personnel' means any person engaged in an activity relating to the loading or unloading of cargo, the movement or tracking of cargo, the maintenance and repair of intermodal equipment, the operation of cargo-related equipment (whether or not integral to the vessel), and the handling of mooring lines on the dock when a vessel is made fast or let go, in the United States or the coastal waters thereof.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (116 Stat. 2135), as amended by section 112, is further amended by inserting after the item relating to section 802 the following:

"Sec. 803. Port security exercise program.".

SEC. 114. RESERVE OFFICERS AND JUNIOR RESERVE OFFICERS TRAINING PILOT PROJECT.

(a) IN GENERAL.—The Secretary of the department in which the Coast Guard is operating (in this section referred to as the "Secretary") may carry out a pilot project to establish and maintain a reserve officers and a junior reserve officers training program in locations determined by the Secretary.

(b) CRITERIA FOR SELECTION.—The Secretary shall establish and maintain a training program under this section in each Coast Guard District, preferably in a location that has a Coast Guard district headquarters. The Secretary shall ensure that at least one program is established at each of an historically black college or university, an hispanic serving institution, and a high school with majority-minority population.

(c) PROGRAM REQUIREMENTS.—A pilot program carried out by the Secretary under this section shall provide students—

(1) instruction in subject areas relating to operations of the Coast Guard; and

(2) training in skills that are useful and appropriate for a career in the Coast Guard.

(d) PROVISION OF ADDITIONAL SUPPORT.—To carry out a pilot program under this section, the Secretary may provide—

(1) assistance in course development, instruction, and other support activities;

(2) commissioned, warrant, and petty officers of the Coast Guard to serve as administrators and instructors; and

(3) necessary and appropriate course materials, equipment, and uniforms.

(e) EMPLOYMENT OF RETIRED COAST GUARD PERSONNEL.—

(1) IN GENERAL.—Subject to paragraph (2), the Secretary may authorize a selected college, university, or high school to employ as administrators and instructors for the pilot program retired Coast Guard and Coast Guard Reserve commissioned, warrant, and petty officers who request that employment and who are approved by the Secretary.

(2) AUTHORIZED PAY.—

(A) IN GENERAL.—Retired members employed pursuant to paragraph (1) may receive their retired or retainer pay and an additional amount of not more than the difference between—

(i) the amount the individual would be paid as pay and allowance if they were considered to have been ordered to active duty with the Coast Guard during that period of employment; and

(ii) the amount of retired pay the individual is entitled to receive during that period.

(B) PAYMENT TO THE SCHOOL.—The Secretary shall pay to a selected college, university, or high school an amount equal to one half of the amount described in subparagraph (A), from funds appropriated for that purpose.

(f) AUTHORIZATION OF APPROPRIATIONS.—To carry out this section there is authorized to be appropriated to the Secretary such sums as may be necessary for each of fiscal years 2007 through 2010.

Subtitle C—Miscellaneous Provisions

SEC. 121. INCREASE IN PORT OF ENTRY INSPECTION OFFICERS.

(a) IN GENERAL.—The Secretary of Homeland Security shall increase by not less than 200 the number of positions for full-time active duty port of entry inspection officers of the Department of Homeland Security for each of the fiscal years 2007 through 2012.

(b) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary to carry out subsection (a) the following amounts for the following fiscal years:

(1) $20,000,000 for fiscal year 2007.

(2) $40,000,000 for fiscal year 2008.

(3) $60,000,000 for fiscal year 2009.

(4) $80,000,000 for fiscal year 2010.

(5) $100,000,000 for fiscal year 2011.

(6) $120,000,000 for fiscal year 2012.

SEC. 122. ACCELERATION OF INTEGRATED DEEPWATER SYSTEM.

In addition to any other amounts authorized by law, there is authorized to be appropriated to the Secretary of Homeland Security $1,892,000,000 for the acquisition and construction of vessels, aircraft, shore and offshore facilities and other components associated with the Integrated Deepwater System in accordance with the report required by section 888 of the Homeland Security Act of 2002 (116 Stat. 2250).

SEC. 123. BORDER PATROL UNIT FOR UNITED STATES VIRGIN ISLANDS.

Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall establish at least one Border Patrol unit for the Virgin Islands of the United States.

SEC. 124. REPORT ON OWNERSHIP AND OPERATION OF UNITED STATES SEAPORTS.

Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the appropriate congressional committees a report that contains—

(1) the name of each individual or entity that leases, operates, manages, or owns real property or facilities at each United States seaport; and

(2) any other information that the Secretary determines to be appropriate.

SEC. 125. REPORT ON SECURITY OPERATIONS AT CERTAIN UNITED STATES SEAPORTS.

(a) STUDY.—The Secretary of Homeland Security shall conduct a study on the adequacy of security operations at the ten United States seaports that load and unload the largest amount of containers.

(b) REPORT.—Not later than 270 days after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees a report on the results of the study required by subsection (a).

SEC. 126. REPORT ON ARRIVAL AND DEPARTURE MANIFESTS FOR CERTAIN COMMERCIAL VESSELS IN THE UNITED STATES VIRGIN ISLANDS.

Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the appropriate congressional committees a report on the impact of implementing the requirements of section 231 of the Immigration and Nationality Act (8 U.S.C. 1221) (relating to providing United States border officers with arrival and departure manifests) with respect to commercial vessels that are fewer than 300 gross tons and operate exclusively between the territorial waters of the United States Virgin Islands and the territorial waters of the British Virgin Islands.

TITLE II—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN

SEC. 201. SECURITY OF THE INTERNATIONAL SUPPLY CHAIN.

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

"TITLE XVIII—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN

"Subtitle A—General Provisions

"SEC. 1801. STRATEGIC PLAN TO ENHANCE THE SECURITY OF THE INTERNATIONAL SUPPLY CHAIN.

"(a) STRATEGIC PLAN.—The Secretary, in consultation with appropriate Federal, State, local, and tribal government agencies and private sector stakeholders responsible for security matters that affect or relate to the movement of containers through the international supply chain, shall develop and implement, and update as appropriate, a strategic plan to enhance the security of the international supply chain.

"(b) REQUIREMENTS.—The strategic plan required under subsection (a) shall—

"(1) describe the roles, responsibilities, and authorities of Federal, State, local, and tribal government agencies and private sector stakeholders that relate to the security of the movement of containers through the international supply chain;

"(2) identify and address gaps and unnecessary overlaps in the roles, responsibilities, or authorities described in paragraph (1);

"(3) identify and make recommendations regarding legislative, regulatory, and organizational changes necessary to improve coordination among the entities or to enhance the security of the international supply chain;

"(4) provide measurable goals, including objectives, mechanisms, and a schedule, for furthering the security of commercial operations from point of origin to point of destination;

"(5) build on available resources and consider costs and benefits;

"(6) provide incentives for additional voluntary measures to enhance cargo security, as determined by the Secretary;

"(7) consider the impact of supply chain security requirements on small and medium size companies;

"(8) include a process for sharing intelligence and information with private sector stakeholders to assist in their security efforts;

"(9) identify a framework for prudent and measured response in the event of a transportation security incident involving the international supply chain;

"(10) provide a plan for the expeditious resumption of the flow of legitimate trade in accordance with section 70103(a)(2)(J)(ii) of title 46, United States Code;

"(11) consider the linkages between supply chain security and security programs within other systems of movement, including travel security and terrorism finance programs; and

"(12) expand upon and relate to existing strategies and plans, including the National Strategy for Maritime Security and the eight supporting plans of the Strategy, as required by Homeland Security Presidential Directive-13 (September 2005).

"(c) UTILIZATION OF ADVISORY COMMITTEES.—As part of the consultations described in subsection (a), the Secretary shall, to the extent practicable, utilize the Homeland Security Advisory Committee, the National Maritime Security Advisory Committee, and the Commercial Operations Advisory Committee to review, as necessary, the draft strategic plan and any subsequent updates to the strategic plan.

"(d) INTERNATIONAL STANDARDS AND PRACTICES.—In furtherance of the strategic plan required under subsection (a), the Secretary is encouraged to consider proposed or established standards and practices of foreign governments and international organizations, including the International Maritime Organization, the World Customs Organization, the International Labor Organization, and the International Organization for Standardization, as appropriate, to establish standards and best practices for the security of containers moving through the international supply chain.

"(e) REPORT.—

"(1) INITIAL REPORT.—The Secretary shall submit to the appropriate congressional committees a report that contains the strategic plan required by subsection (a).

"(2) FINAL REPORT.—Not later than three years after the date on which the strategic plan is submitted under paragraph (1), the Secretary shall submit to the appropriate congressional committees a report that contains an update of the strategic plan.

"(f) DEFINITION.—In this section, the term 'transportation security incident' has the meaning given the term in section 70101(6) of title 46, United States Code.

"SEC. 1802. TRANSMISSION OF ADDITIONAL DATA ELEMENTS FOR IMPROVED HIGH RISK TARGETING.

"(a) REQUIREMENT.—The Secretary shall require transmission to the Department, through an electronic data interchange system, of additional data elements for improved high risk targeting, including appropriate security elements of entry data, as determined by the Secretary, to be provided as advanced information with respect to cargo destined for importation into the United States prior to loading of such cargo on vessels at foreign seaports.

"(b) REGULATIONS.—The Secretary shall promulgate regulations to carry out this section. In promulgating such regulations, the Secretary shall adhere to the parameters applicable to the development of regulations under section 343(a) of the Trade Act of 2002 (19 U.S.C. 2071 note), including provisions relating to consultation, technology, analysis, use of information, confidentiality, and timing requirements.

"SEC. 1803. PLAN TO IMPROVE THE AUTOMATED TARGETING SYSTEM.

"(a) PLAN.—The Secretary shall develop and implement a plan to improve the Automated Targeting System for the identification of high-risk containers moving through the international supply chain.

"(b) CONTENTS.—

"(1) TREATMENT OF RECOMMENDATIONS.—The Secretary shall include in the plan required under subsection (a) a schedule to address the recommendations of the Comptroller General of the United States, the Inspector General of the Department of the Treasury, and the Inspector General of the Department of Homeland Security with respect to the operation of the Automated Targeting System.

"(2) INFORMATION SUBMISSIONS.—In developing the plan required under subsection (a), the Secretary shall consider the cost, benefit, and feasibility of—

"(A) requiring additional nonmanifest documentation for each container;

"(B) adjusting the time period allowed by law for revisions to a container cargo manifest;

"(C) adjusting the time period allowed by law for submission of entry data for vessel or cargo; and

"(D) such other actions the Secretary considers beneficial for improving the information relied upon for the Automated Targeting System and any other targeting systems in furthering the security and integrity of the international supply chain.

"(3) OUTSIDE REVIEW.—The Secretary shall conduct, through an independent panel, a review of the Automated Targeting System. The results of this review shall be included in the plan required under subsection (a).

"(4) SMART SYSTEM.—The Secretary shall consider future iterations of the Automated Targeting System, which would incorporate smart features, such as more complex algorithms and real-time intelligence, instead of relying solely on rule sets that are periodically updated. The Secretary shall also consider how the Automated Targeting System could be improved through linkages with targeting systems in existence on the date of the enactment of the Security and Accountability For Every Port Act for travel security and terrorism finance programs.

"(c) NEW OR EXPANDED INFORMATION SUBMISSIONS.—In considering any new or expanded information submission requirements, the Secretary shall consult with stakeholders and identify the need for such information, appropriate confidentiality requirements with respect to such information, and appropriate timing of the submission of such information, in the plan required under subsection (a).

"(d) SECURE TRANSMISSION OF CERTAIN INFORMATION.—All information required by the Department from supply chain partners shall be transmitted in a secure fashion, as determined by the Secretary, so as to protect the information from unauthorized access.

"(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated $5,000,000 for each of the fiscal years 2007 through 2012 to carry out this section.

"SEC. 1804. CONTAINER STANDARDS AND VERIFICATION PROCEDURES.

"(a) ESTABLISHMENT.—

"(1) IN GENERAL.—The Secretary shall establish minimum standards and verification procedures for securing containers in transit to the United States relating to the sealing of containers.

"(2) DEADLINE FOR ENFORCEMENT.—Not later than two years after the date on which the standards and procedures are established pursuant to paragraph (1), all containers bound for ports of entry in the United States shall meet such standards and procedures.

"(b) REVIEW AND ENHANCEMENT.—The Secretary shall regularly—

"(1) review the standards and procedures established pursuant to subsection (a); and

"(2) enhance the security standards and procedures, as appropriate, based on tests of technologies as they become commercially available to detect container intrusion and the highest consequence threats, particularly weapons of mass destruction.

"(c) INTERNATIONAL CARGO SECURITY STANDARDS.—The Secretary, in consultation with the Secretary of State, is encouraged to promote and establish international standards for the security of containers moving through the international supply chain with foreign governments and international organizations, including the International Maritime Organization and the World Customs Organization.

"(d) INTERNATIONAL TRADE AND OTHER OBLIGATIONS.—In carrying out this section, the Secretary shall consult with appropriate Federal departments and agencies and private sector stakeholders to ensure that actions under this section do not violate international trade obligations or other international obligations of the United States.

"SEC. 1805. CONTAINER SECURITY INITIATIVE (CSI).

"(a) AUTHORIZATION.—The Secretary is authorized to establish and implement a program (to be known as the 'Container Security Initiative' or 'CSI') to identify and examine maritime containers that pose a risk for terrorism at foreign ports before the containers are shipped to the United States.

"(b) ASSESSMENT.—Before the Secretary designates any foreign port under CSI, the Secretary, in consultation with other Federal officials, as appropriate, shall conduct an assessment of the port, including—

"(1) the level of risk for the potential compromise of containers by terrorists or terrorist weapons;

"(2) the volume of regular container traffic to United States ports;

"(3) the results of the Coast Guard assessments conducted pursuant to section 70108 of title 46, United States Code;

"(4) the commitment of the host nation to cooperating with the Department in sharing critical data and risk management information and to maintain programs to ensure employee integrity; and

"(5) the potential for validation of security practices by the Department.

"(c) NOTIFICATION.—The Secretary shall notify the appropriate congressional committees prior to notifying the public of the designation of a foreign port under CSI.

"(d) INSPECTIONS.—

"(1) REQUIREMENTS AND PROCEDURES.—The Secretary shall—

"(A) establish technical capability criteria and standard operating procedures for the use of nonintrusive inspection and nuclear and radiological detection systems in conjunction with CSI;

"(B) require each port designated under CSI to operate nonintrusive inspection and nuclear and radiological detection systems in accordance with the technical capability criteria and standard operating procedures established under subparagraph (A); and

"(C) continually monitor the technologies, processes, and techniques used to inspect cargo at ports designated under CSI.

"(2) CONSISTENCY OF STANDARDS AND PROCEDURES.—The Secretary shall ensure that the technical capability criteria and standard operating procedures established under paragraph (1)(A) are consistent with such standards and procedures of any other department or agency of the Federal government with respect to deployment of nuclear and radiological detection systems outside the United States.

"(3) FOREIGN ASSISTANCE.—

"(A) IN GENERAL.—The Secretary, in consultation with the Secretary of State, the Secretary of Energy, and the heads of other Federal agencies, shall identify foreign assistance programs that could facilitate the implementation of cargo security antiterrorism measures at ports designated under CSI and foreign ports not designated under CSI that lack effective antiterrorism measures.

"(B) ACQUISITION.—The Secretary is authorized to loan or otherwise assist in the deployment of nonintrusive inspection or nuclear and radiological detection systems for cargo containers at each designated CSI port under such terms and conditions as the Secretary determines to be appropriate and to provide training for foreign personnel involved in CSI.

"(e) PROHIBITION.—

"(1) IN GENERAL.—The Secretary shall issue a 'do not load' order to each port designated under CSI to prevent the onload of any cargo that has been identified as higher risk by the Automated Targeting System unless the cargo—

"(A) is scanned with a non intrusive imagery device and nuclear or radiological detection equipment;

"(B) is devanned and inspected with nuclear or radiological detection equipment; or

"(C) is determined to be of lower risk following additional inquiries by appropriate personnel of U.S. Customs and Border Protection.

"(2) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to interfere with the ability of the Secretary to deny entry of any cargo into the United States.

"(f) REPORT.—The Secretary shall submit to the appropriate congressional committees not later than March 1 of each year a report on the status of CSI, including—

"(1) a description of the security improvements gained through CSI;

"(2) the rationale for the continuance of each port designated under CSI;

"(3) an assessment of the personnel needs at each port designated under CSI; and

"(4) a description of the potential for remote targeting to decrease the number of personnel who are deployed at foreign ports under CSI.

"(g) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated $196,000,000 for each of the fiscal years 2007 through 2012 to carry out this section.

"SEC. 1806. INFORMATION SHARING RELATING TO SUPPLY CHAIN SECURITY COOPERATION.

"(a) PURPOSES.—The purposes of this section are—

"(1) to establish continuing liaison and to provide for supply chain security cooperation between Department and the private sector; and

"(2) to provide for regular and timely interchange of information between the private sector and the Department concerning developments and security risks in the supply chain environment.

"(b) SECURE SYSTEM.—The Secretary shall develop a secure electronic data interchange system to collect from and share appropriate risk information related to securing the supply chain with the private sector entities determined appropriate by the Secretary.

"(c) CONSULTATION.—In developing the system under subsection (b), the Secretary shall consult with the Commercial Operations Advisory Committee and a broad range of public and private sector entities likely to utilize the system, including importers, exporters, carriers, customs brokers, and freight forwarders, among other parties.

"(d) PROCEDURES.—The Secretary shall establish uniform procedures for the receipt, care, and storage of supply chain security information that is voluntarily submitted to the Department through the system developed under subsection (b).

"(e) LIMITATIONS.—The voluntary information collected through the system developed under subsection (b) shall be used exclusively for ensuring security and shall not be used for determining entry or for any other commercial enforcement purpose. The voluntary information submitted to the Department through the system developed under subsection (b) shall not be construed to constitute compliance with any requirement to submit such information to a Federal agency under any other provision of law.

"(f) PARTICIPANTS.—The Secretary shall develop protocols for determining appropriate private sector personnel who shall have access to the system developed under subsection (b). Such personnel shall include designated security officers within companies that are determined to be low risk through participation in the Customs-Trade Partnership Against Terrorism program established pursuant to subtitle B of this title.

"(g) CONFIDENTIALITY.—Notwithstanding any other provision of law, information that is voluntarily submitted by the private sector to the Department through the system developed under subsection (b)—

"(1) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act);

"(2) shall not, without the written consent of the person or entity submitting such information, be used directly by the Department or a third party, in any civil action arising under Federal or State law if such information is submitted in good faith; and

"(3) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this section, except—

"(A) in furtherance of an investigation or other prosecution of a criminal act; or

"(B) when disclosure of the information would be—

"(i) to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

"(ii) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the Comptroller General.

"(h) INDEPENDENTLY OBTAINED INFORMATION.—Nothing in this section shall be construed to limit or otherwise affect the ability of a Federal, State, or local, government entity, under applicable law, to obtain supply chain security information, including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law.

"(i) PENALTIES.—Whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any supply chain security information protected in this section from disclosure, shall be fined under title 18, United States Code, imprisoned not more than 1 year, or both, and shall be removed from office or employment.

"(j) AUTHORITY TO ISSUE WARNINGS.—The Secretary may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential risks to the supply chain as appropriate. In issuing a warning, the Secretary shall take appropriate actions to protect from disclosure—

"(1) the source of any voluntarily submitted supply chain security information that forms the basis for the warning; and

"(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

"Subtitle B—Customs-Trade Partnership Against Terrorism (C-TPAT)

"SEC. 1811. ESTABLISHMENT.

"(a) ESTABLISHMENT.—The Secretary is authorized to establish a voluntary program (to be known as the 'Customs-Trade Partnership Against Terrorism' or 'C–TPAT') to strengthen and improve the overall security of the international supply chain and United States border security.

"(b) MINIMUM SECURITY REQUIREMENTS.—The Secretary shall review the minimum security requirements of C–TPAT at least once every year and update such requirements as necessary.

"SEC. 1812. ELIGIBLE ENTITIES.

"Importers, brokers, forwarders, air, sea, land carriers, and other entities in the international supply chain and intermodal transportation system are eligible to apply to voluntarily enter into partnerships with the Department under C-TPAT.

"SEC. 1813. MINIMUM REQUIREMENTS.

"An applicant seeking to participate in C–TPAT shall—

"(1) demonstrate a history of moving commerce in the international supply chain;

"(2) conduct an assessment of its supply chains based upon security criteria established by the Secretary, including—

"(A) business partner requirements;

"(B) container security;

"(C) physical security and access controls;

"(D) personnel security;

"(E) procedural security;

"(F) security training and threat awareness; and

"(G) information technology security;

"(3) implement and maintain security measures and supply chain security practices meeting security criteria; and

"(4) meet all other requirements established by the Secretary.

"SEC. 1814. TIER ONE PARTICIPANTS.

"(a) BENEFITS.—The Secretary may offer limited benefits to C–TPAT participants whose security measures and supply chain security practices have been certified in accordance with the guidelines established pursuant to subsection (b).

"(b) GUIDELINES.—The Secretary shall update guidelines for certifying a C-TPAT participant's security measures and supply chain security practices under this section.

"SEC. 1815. TIER TWO PARTICIPANTS.

"(a) IN GENERAL.—Not later than one year after a C-TPAT participant has been certified under section 1814, the Secretary shall validate, directly or through third party entities certified in accordance with section 1817, the security measures and supply chain security practices of that participant. Such validation shall include assessments at appropriate foreign locations utilized by the participant as part of the supply chain.

"(b) CONSEQUENCES FOR FAILED VALIDATION.—If a C–TPAT participant's security measures and supply chain security practices fail to meet the validation requirements under this section, the Commissioner of U.S. Customs and Border Protection may—

"(1) deny the participant benefits under C–TPAT on a temporary or permanent basis; or

"(2) suspend or expel the participant from C–TPAT.

"(c) RIGHT OF APPEAL.—A C–TPAT participant described in subsection (b) may file an appeal with the Secretary of the Commissioner's decision under subsection (b)(1) to deny benefits under C–TPAT or under subsection (b)(2) to suspend or expel the participant from C–TPAT.

"(d) BENEFITS.—The Secretary shall extend benefits to each C-TPAT participant that has been validated under this section, which may include—

"(1) reduced examinations; and

"(2) priority processing for searches.

"SEC. 1816. TIER THREE PARTICIPANTS.

"(a) IN GENERAL.—The Secretary shall establish a third tier of C-TPAT that offers additional benefits to C-TPAT participants that demonstrate a sustained commitment beyond the minimum criteria for participation in C-TPAT.

"(b) ADDITIONAL CRITERIA.—The Secretary shall designate criteria for C-TPAT participants under this section that may include criteria to ensure—

"(1) cargo is loaded on a vessel with a vessel security plan approved under section 70103(c) of title 46, United States Code, or on a vessel with a valid International Ship Security Certificate as provided for under part 104 of title 33, Code of Federal Regulations;

"(2) container security devices and related policies and practices that exceed the standards and procedures established by the Secretary are utilized; and

"(3) cargo complies with any other requirements determined by the Secretary.

"(c) BENEFITS.—The Secretary, in consultation with the Commercial Operations Advisory Committee and the National Maritime Security Advisory Committee, may provide benefits to C-TPAT participants under this section, which may include—

"(1) the expedited release of tier three cargo into destination ports within the United States during all threat levels designated by the Secretary;

"(2) reduced or streamlined bonding requirements that are consistent with obligations under other applicable provisions of law;

"(3) preference to vessels;

"(4) further reduced examinations;

"(5) priority processing for examinations;

"(6) further reduced scores in the Automated Targeting System; and

"(7) streamlined billing of any customs duties or fees.

"(d) DEFINITION.—In this section, the term 'container security device' means a mechanical or electronic device designed to, at a minimum, detect unauthorized intrusion of containers.

"SEC. 1817. CONSEQUENCES FOR LACK OF COMPLIANCE.

"(a) IN GENERAL.—If a C–TPAT participant's security measures and supply chain security practices fail to meet any of the requirements under this subtitle, the Secretary may deny the participant benefits in whole or in part under this subtitle.

"(b) FALSE OR MISLEADING INFORMATION.—If a C-TPAT participant intentionally provides false or misleading information to the Secretary or a third party entity during the validation process of the participant under this subtitle, the Commissioner of U.S. Customs and Border Protection shall suspend or expel the participant from C-TPAT for a period of not less than five years.

"(c) RIGHT OF APPEAL.—A C–TPAT participant described in subsection (a) may file an appeal with the Secretary of the Secretary's decision under subsection (a) to deny benefits under this subtitle. A C-TPAT participant described in subsection (b) may file an appeal with the Secretary of the Commissioner's decision under subsection (b) to suspend or expel the participant from C-TPAT.

"SEC. 1818. VALIDATIONS BY THIRD PARTY ENTITIES.

"(a) IN GENERAL.—In conducting the pilot program under subsection (f), and if the Secretary determines to expand the use of third party entities to conduct validations of C-TPAT participants upon completion of the pilot program under subsection (f), the Secretary shall—

"(1) develop, document, and update, as necessary, minimum standard operating procedures and requirements applicable to such entities for the conduct of such validations; and

"(2) meet all requirements under subtitle G of the title VIII of this Act to review and designate such minimum standard operating procedures as a qualified anti-terrorism technology for purposes of such subtitle.

"(b) CERTIFICATION OF THIRD PARTY ENTITIES.—

"(1) ISSUANCE OF CERTIFICATE OF CONFORMANCE.—In accordance with section 863(d)(3) of this Act, the Secretary shall issue a certificate of conformance to a third party entity to conduct validations under this subtitle if the entity—

"(A) demonstrates to the satisfaction of the Secretary the ability to perform validations in accordance with standard operating procedures and requirements (or updates thereto) designated as a qualified anti-terrorism technology by the Secretary under subsection (a); and

"(B) agrees—

"(I) to perform validations in accordance with such standard operating procedures and requirements (or updates thereto); and

"(ii) to maintain liability insurance coverage at policy limits and in accordance with conditions to be established by the Secretary pursuant to section 864 of this Act; and

"(C) signs an agreement to protect all proprietary information of C-TPAT participants with respect to which the entity will conduct validations.

"(2) LITIGATION AND RISK MANAGEMENT PROTECTIONS.—A third party entity that maintains liability insurance coverage at policy limits and in accordance with conditions to be established by the Secretary pursuant to section 864 of this Act and receives a certificate of conformance under paragraph (1) shall receive all applicable litigation and risk management protections under sections 863 and 864 of this Act.

"(3) RECIPROCAL WAIVER OF CLAIMS.—A reciprocal waiver of claims shall be deemed to have been entered into between a third party entity that receives a certificate of conformance under paragraph (1) and its contractors, subcontractors, suppliers, vendors, customers, and contractors and subcontractors of customers involved in the use or operation of the validation services of the third party entity.

"(c) INFORMATION FOR ESTABLISHING LIMITS OF LIABILITY INSURANCE.—A third party entity seeking a certificate of conformance under subsection (b)(1) shall provide to the Secretary necessary information for establishing the limits of liability insurance required to be maintained by the entity under section 864(a) of this Act.

"(d) ADDITIONAL REQUIREMENTS.—The Secretary shall ensure that—

"(1) any third party entity under this section—

"(A) has no beneficial interest in or any direct or indirect control over the C-TPAT participant that is contracting for the validation services; and

"(B) has no other conflict of interest with respect to the C-TPAT participant; and

"(2) the C-TPAT participant has entered into a contract with the third party entity under which the C-TPAT participant agrees to pay all costs associated with the validation.

"(e) MONITORING.—

"(1) IN GENERAL.—The Secretary shall regularly monitor and inspect the operations of a third party entity conducting validations under this subtitle to ensure that the entity is meeting the minimum standard operating procedures and requirements for the validation of C-TPAT participants established under subsection (a) and all other applicable requirements for validation services under this subtitle.

"(2) REVOCATION.—If the Secretary finds that a third party entity is not meeting the minimum standard operating procedures and requirements, the Secretary shall—

"(A) revoke the entity's certificate of conformance issued under subsection (b)(1); and

"(B) review any validations conducted by the entity.

"(f) PILOT PROGRAM.—

"(1) IN GENERAL.—The Secretary shall carry out a pilot program to test the feasibility, costs, and benefits of utilizing third party entities to conduct validations of C-TPAT participants. In conducting the pilot program, the Secretary shall comply with all applicable requirements of this section with respect to eligibility of third party entities to conduct validations of C-TPAT participants.

"(2) REPORT.—Not later than 30 days after the completion of the pilot program conducted pursuant to paragraph (1), the Secretary shall submit to the appropriate congressional committees a report that contains—

"(A) the results of the pilot program; and

"(B) the determination of the Secretary whether or not to expand the use of third party entities to conduct validations of C-TPAT participants.

"SEC. 1819. REVALIDATION.

"The Secretary shall establish a process for revalidating C-TPAT participants under this subtitle. Such revalidation shall occur not less frequently than once during every 3-year period following the initial validation.

"SEC. 1820. NON-CONTAINERIZED CARGO.

"The Secretary may consider the potential for participation in C-TPAT by importers of non-containerized cargoes that otherwise meet the requirements under this subtitle.

"SEC. 1821. AUTHORIZATION OF APPROPRIATIONS.

"There are authorized to be appropriated $75,000,000 for each of the fiscal years 2007 through 2012 to carry out this subtitle.

"Subtitle C—Miscellaneous Provisions

"SEC. 1831. RESEARCH, DEVELOPMENT, TEST, AND EVALUATION EFFORTS IN FURTHERANCE OF MARITIME AND CARGO SECURITY.

"(a) IN GENERAL.—The Secretary shall—

"(1) direct research, development, test, and evaluation efforts in furtherance of maritime and cargo security;

"(2) encourage the ingenuity of the private sector in developing and testing technologies and process innovations in furtherance of these objectives; and

"(3) evaluate such technologies.

"(b) COORDINATION.—The Secretary, in coordination with the Undersecretary for Science and Technology, the Director of the Domestic Nuclear Detection Office of the Department, and the heads of other appropriate offices or entities of the Department, shall ensure that—

"(1) research, development, test, and evaluation efforts funded by the Department in furtherance of maritime and cargo security are coordinated to avoid duplication of efforts; and

"(2) the results of such efforts are shared throughout the Department and other Federal, State, and local agencies, as appropriate.

"SEC. 1832. GRANTS UNDER OPERATION SAFE COMMERCE.

"(a) IN GENERAL.—The Secretary shall provide grants, as part of Operation Safe Commerce, to—

"(1) integrate nonintrusive imaging inspection and nuclear and radiological detection systems with automatic identification methods for containers, vessels, and vehicles;

"(2) test physical access control protocols and technologies to include continuous tracking devices that provide real-time monitoring and reporting;

"(3) create a data sharing network capable of transmitting data required by entities participating in the international supply chain from every intermodal transfer point to the National Targeting Center of the Department; and

"(4) otherwise further maritime and cargo security, as determined by the Secretary.

"(b) SUPPLY CHAIN SECURITY FOR SPECIAL CONTAINER AND NONCONTAINERIZED CARGO.—In providing grants under subsection (a), the Secretary shall establish demonstration projects that further the security of the international supply chain, including refrigerated containers, and noncontainerized cargo, including roll-on/roll-off, break-bulk, liquid, and dry bulk cargo, through real-time, continuous tracking technology for special or high-risk container cargo that poses unusual potential for human or environmental harm.

"(c) COMPETITIVE SELECTION PROCESS.—The Secretary shall select recipients of grants under subsection (a) through a competitive process on the basis of the following criteria:

"(1) The extent to which the applicant can demonstrate that personnel, laboratory, and organizational resources will be available to the applicant to carry out the activities authorized under this section.

"(2) The applicant's capability to provide leadership in making national and regional contributions to the solution of maritime and cargo security issues.

"(3) The extent to which the applicant's programs, projects, and activities under the grant will address highest risk priorities as determined by the Secretary.

"(4) The extent to which the applicant has a strategic plan for carrying out the programs, projects, and activities under the grant.

"(5) Any other criteria the Secretary determines to be appropriate.

"(d) ADMINISTRATIVE PROVISIONS.—

"(1) PROHIBITION ON DUPLICATION OF EFFORT.—Before providing any grant under subsection (a), the Secretary shall coordinate with other Federal departments and agencies to ensure the grant will not duplicate work already being carried out with Federal funding.

"(2) ACCOUNTING, REPORTING, AND REVIEW PROCEDURES.—The Secretary shall establish accounting, reporting, and review procedures to ensure that—

"(A) amounts made available under a grant provided under subsection (a)—

"(i) are used for the purpose for which such amounts were made available; and

"(ii) are properly accounted for; and

"(B) amounts not used for such purpose and amounts not expended are recovered.

"(3) RECORDKEEPING.—The recipient of a grant under subsection (a) shall keep all records related to expenditures and obligations of amounts provided under the grant and make such records available upon request to the Secretary for audit and examination.

"(4) REVIEW.—The Secretary shall annually review the programs, projects, and activities carried out using amounts made available under grants provided under subsection (a) to ensure that obligations and expenditures of such amounts are consistent with the purposes for which such amounts are made available.

"(e) ANNUAL REPORT.—Not later than March 1 of each year, the Secretary shall submit to the appropriate congressional committees a report detailing the results of Operation Safe Commerce.

"(f) DEFINITION.—In this section, the term 'Operation Safe Commerce' means the research, development, test, and evaluation grant program that brings together private sector shareholders, port officials, and Federal, State, and local representatives

to analyze existing security procedures for cargo and develop new security protocols that have the potential to increase the security of cargo shipments by monitoring the movement and integrity of cargo through the international supply chain.

"(g) AUTHORIZATION OF APPROPRIATIONS.—

"(1) IN GENERAL.—Subject to paragraph (2), there are authorized to be appropriated $25,000,000 for each of fiscal years 2007 through 2012 to carry out this section.

"(2) EFFECTIVE DATE.—Paragraph (1) shall be effective beginning on the date on which the Secretary submits to the appropriate congressional committees a report on the implementation and results of grants provided under Operation Safe Commerce before the date of the enactment of the Security and Accountability For Every Port Act.

"SEC. 1833. DEFINITIONS.

"In this title, the following definitions apply:

"(1) AUTOMATED TARGETING SYSTEM.—The term 'Automated Targeting System' means the rules-based system incorporating intelligence material and import transaction history, established by U.S. Customs and Border Protection to target high risk shipments of cargo.

"(2) EXAMINATION.—The term 'examination' means a physical inspection or the imaging and radiation screening of a conveyance using non-intrusive inspection (NII) technology, for the presence of contraband.

"(3) INSPECTION.—The term 'inspection' means the comprehensive process used by U.S. Customs and Border Protection for assessing goods entering the United States to appraise them for duty purposes, to detect the presence of restricted or prohibited items, and to ensure compliance with all applicable laws. This process may include screening, conducting an examination, or conducting a search.

"(4) INTERNATIONAL SUPPLY CHAIN.—The term 'international supply chain' means the end-to-end process for shipping goods from a point of origin overseas to and from the United States.

"(5) NUCLEAR AND RADIOLOGICAL DETECTION SYSTEM.—The term 'nuclear and radiological detection system' means any technology that is capable of detecting or identifying nuclear and radiological material or explosive devices.

"(6) SCREENING.—The term 'screening' means a visual or automated review of information about goods, including manifest or entry documentation accompanying a shipment being imported into the United States, to determine or assess the threat of such cargo.

"(7) SEARCH.—The term 'search' means an intrusive examination in which a container is opened and its contents are de-vanned and visually inspected for the presence of misdeclared, restricted, or prohibited items.".

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

"TITLE XVIII—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN

"Subtitle A—General Provisions

"Sec. 1801. Strategic plan to enhance the security of the international supply chain.
"Sec. 1802. Transmission of additional data elements for improved high risk targeting.
"Sec. 1803. Plan to improve the Automated Targeting System.
"Sec. 1804. Container standards and verification procedures.
"Sec. 1805. Container Security Initiative (CSI).
"Sec. 1806. Information sharing relating to supply chain security cooperation.

"Subtitle B—Customs-Trade Partnership Against Terrorism (C-TPAT)

"Sec. 1811. Establishment.
"Sec. 1812. Eligible entities.
"Sec. 1813. Minimum requirements.
"Sec. 1814. Tier one participants.
"Sec. 1815. Tier two participants.
"Sec. 1816. Tier three participants.
"Sec. 1817. Consequences for lack of compliance.
"Sec. 1818. Validations by third party entities.
"Sec. 1819. Revalidation.
"Sec. 1820. Non-containerized cargo.
"Sec. 1821. Authorization of appropriations.

"Subtitle C—Miscellaneous Provisions

"Sec. 1831. Research, development, test, and evaluation efforts in furtherance of maritime and cargo security.
"Sec. 1832. Grants under Operation Safe Commerce.
"Sec. 1833. Definitions.".

(c) EFFECTIVE DATES.—The Secretary of Homeland Security shall—

(1) submit to the appropriate congressional committees the report required by section 1801(e)(1) of the Homeland Security Act of 2002, as added by subsection (a), not later than 180 days after the date of enactment of this Act;

(2) promulgate regulations under section 1802(b) of the Homeland Security Act of 2002, as added by subsection (a), not later than one year after the date of the enactment of this Act;

(3) develop and implement the plan to improve the Automated Targeting System under section 1803(a) of the Homeland Security Act of 2002, as added by subsection (a), not later than 180 days after the date of the enactment of this Act,

(4) develop the standards and verification procedures described in section 1804(a)(1) of the Homeland Security Act of 2002, as added by subsection (a), not later than 180 days after the date of the enactment of this Act;

(5) begin exercising authority to issue a "do not load" order to each port designated under CSI pursuant to section 1805(e) of the Homeland Security Act of 2002, as added by subsection (a), not later than 180 days after the date of the enactment of this Act;

(6) develop the secure electronic data interchange system under section 1806(b) of the Homeland Security Act of 2002, as added by subsection (a), not later than one year after the date of the enactment of this Act;

(7) update guidelines for certifying a C-TPAT participant's security measures and supply chain security practices under section 1814(b) of the Homeland Security Act of 2002, as added by subsection (a), not later than 180 days after the date of the enactment of this Act;

(8) develop a schedule and update guidelines for validating a C-TPAT participant's security measures and supply chain security practices under section 1815 of the Homeland Security Act of 2002, as added by subsection (a), not later than 180 days after the date of enactment of this Act;

(9) provide appropriate benefits described in subsection (d) of section 1816 of the Homeland Security Act of 2002, as added by subsection (a), to C-TPAT participants under section 1816 of such Act beginning not later than two years after the date of the enactment of this Act; and

(10) carry out the pilot program described in section 1818(f) of the Homeland Security Act of 2002, as added by subsection (a), beginning not later than one year after the date of the enactment of this Act for a duration of not less than a one-year period.

SEC. 202. NEXT GENERATION SUPPLY CHAIN SECURITY TECHNOLOGIES.

(a) EVALUATION OF EMERGING TECHNOLOGIES.—While maintaining the current layered, risk-based approach to screening, scanning, and inspecting cargo at foreign ports bound for the United States in accordance with existing statutory provisions, the Secretary of Homeland Security shall evaluate the development of nuclear and radiological detection systems and other inspection technologies for use at foreign seaports to increase the volume of containers scanned prior to loading on vessels bound for the United States.

(b) EMERGING TECHNOLOGY.—Not later than one year after the date of the enactment of this Act, the Secretary shall, having evaluated emerging technologies under subsection (a), determine if more capable, commercially available technology exists, and whether such technology—

(1) has a sufficiently low false alarm rate for use in the supply chain;

(2) is capable of being deployed and operated at ports overseas;

(3) is capable of integrating, where necessary, with existing systems;

(4) does not significantly impact trade capacity and flow of cargo at foreign or United States ports; and

(5) provides an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.

(c) CONTINGENT IMPLEMENTATION.—If the Secretary determines the available technology meets the criteria outlined in subsection (b), the Secretary, in cooperation with the Secretary of State, shall within 180 days of such determination, seek to secure the cooperation of foreign governments to initiate and maximize the use of such technology at foreign ports to scan all cargo possible.

(d) INTERNATIONAL COOPERATION.—If the Secretary determines that a proposed technology meets the requirements of subsection (b), but cannot be implemented as a result of a foreign government's refusal to cooperate in the phased deployment, the Secretary may refuse to accept containerized cargo from that port.

(e) REPORT.—The Secretary shall submit to the appropriate congressional committees on an annual basis a report on the evaluation performed under subsections (a) and (b), the status of any implementation initiated in accordance with subsection (c), and a detailed assessment of the level of cooperation of foreign governments, as well as any actions taken by the Secretary under subsection (d).

(f) DEFINITION.—In this section, the term "nuclear and radiological detection system" means any technology that is capable of detecting or identifying nuclear and radiological material or explosive devices.

SEC. 203. UNIFORM DATA SYSTEM FOR IMPORT AND EXPORT INFORMATION.

(a) ESTABLISHMENT.—The President shall establish and implement a single, uniform data system for the electronic collection, dissemination, and sharing of import and export information to increase the efficiency of data submission and the security of such data related to border security, trade, and public health and safety of international cargoes.

(b) PRIVATE SECTOR CONSULTATION.—The President shall consult with private sector stakeholders in developing uniform data submission requirements, procedures, and schedules under the system established pursuant to subsection (a).

(c) REPORT.—Not later than 120 days after the date of the enactment of this Act, the President shall transmit to the appropriate congressional committees a report on the schedule for full implementation of the system established pursuant to subsection (a).

(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to prevent any Federal department or agency from collecting import and export information under any other provision of law.

SEC. 204. FOREIGN PORT ASSESSMENTS.

Section 70108 of title 46, United States Code, is amended by adding at the end the following:

"(d) PERIODIC REASSESSMENT.—The Secretary, acting through the Commandant of the Coast Guard, shall reassess the effectiveness of antiterrorism measures maintained at ports as described under subsection (a) and of procedures described in subsection (b) not less than every 3 years.".

SEC. 205. PILOT PROGRAM TO IMPROVE THE SECURITY OF EMPTY CONTAINERS.

(a) IN GENERAL.—The Secretary of Homeland Security shall conduct a one-year pilot program to evaluate and improve the security of empty containers at United States seaports to ensure the safe and secure delivery of cargo and to prevent potential acts of terrorism involving such containers. The pilot program shall include the use of visual searches of empty containers at United States seaports.

(b) REPORT.—Not later than 90 days after the completion of the pilot program under paragraph (1), the Secretary shall prepare and submit to the appropriate congressional committees a report that contains—

(1) the results of pilot program; and

(2) the determination of the Secretary whether or not to expand the pilot program.

SEC. 206. STUDY AND REPORT ON ADVANCED IMAGERY PILOT PROGRAMS.

(a) STUDY.—

(1) IN GENERAL.—The Secretary of Homeland Security, in consultation with the Commissioner of U.S. Customs and Border Protection, shall conduct a study of the merits of current container inspection pilot programs which include nuclear or radiological detection, non-intrusive imagery, and density scanning capabilities.

(2) REQUIREMENTS.—The study required under paragraph (1) shall include, at a minimum—

(A) an evaluation of the cost, personnel, and infrastructure required to operate the pilot programs, as well as the cost, personnel, and infrastructure required to move the pilot programs into full-scale deployment to screen all cargo imported from foreign ports;

(B) an evaluation of the cost, personnel, and infrastructure required by U.S. Customs and Border Protection to validate the data generated from the pilot programs;

(C) a summary of best practices and technological advances of the pilot programs that could be integrated into the Container Security Initiative and other container security programs; and

(D) an assessment of the impact of technology or processes utilized in the pilot programs on improving cargo operations and security.

(b) REPORT.—Not later than 60 days after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees a report that contains—

(1) the results of the study required under subsection (a); and

(2) recommendations to improve container security programs within the Department of Homeland Security.

TITLE III—DIRECTORATE FOR POLICY, PLANNING, AND INTERNATIONAL AFFAIRS

SEC. 301. ESTABLISHMENT OF DIRECTORATE.

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

(1) by redesignating title VI as title XIX, and moving such title so as to appear after title XVIII, as added by section 201;

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

"TITLE XIX—MISCELLANEOUS PROVISIONS".

(3) by redesignating section 601 as section 1901; and

(4) by inserting after title V the following new title:

"TITLE VI—POLICY, PLANNING, AND INTERNATIONAL AFFAIRS

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

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

"(b) UNDER SECRETARY FOR POLICY.—

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

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

"(c) RESPONSIBILITIES OF UNDER SECRETARY.—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"(i) the exchange of information on research and development on homeland security technologies;

"(ii) joint training exercises of first responders in coordination with the Assistant Secretary for Grants and Training; and

"(iii) exchanging expertise and information on terrorism prevention, response, and crisis management.

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

"(C) To plan and participate in international conferences, exchange programs (including the exchange of scientists, engineers, and other experts), and other training activities with friendly nations

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

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

"(F) To represent the Department in international negotiations, working groups, and standards-setting bodies.

"(4) PRIVATE SECTOR.—

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

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

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

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

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

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

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

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

"SEC. 602. OFFICE OF INTERNATIONAL AFFAIRS.

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

"(b) DUTIES OF THE ASSISTANT SECRETARY.—The Assistant Secretary shall have the following duties:

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

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

"(B) Joint training exercises of first responders.

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

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

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

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

"SEC. 603. OTHER OFFICES AND OFFICIALS.

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

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

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

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

"(B) a Screening Coordination and Operations Office.

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

"(4) The Victim Assistance Officer.

"(5) The Tribal Security Officer.

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

"(b) DIRECTOR OF CARGO SECURITY POLICY.—

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

"(2) RESPONSIBILITIES.—The Director shall—

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

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

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

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

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

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

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

"TITLE VI—POLICY, PLANNING, AND INTERNATIONAL AFFAIRS

"Sec. 601. Directorate for Policy, Planning, and International Affairs.
"Sec. 602. Office of International Affairs.
"Sec. 603. Other offices and officials."

(3) by inserting after the items relating to title XVIII the following:

"TITLE XIX—MISCELLANEOUS PROVISIONS

"Sec. 1901. Treatment of charitable trusts for members of the armed forces of the United States and other governmental organizations.".

TITLE IV—OFFICE OF DOMESTIC NUCLEAR DETECTION

SEC. 401. ESTABLISHMENT OF OFFICE.

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

"TITLE XX—OFFICE OF DOMESTIC NUCLEAR DETECTION

"SEC. 2001. DOMESTIC NUCLEAR DETECTION OFFICE.

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

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

"(c) DIRECTOR.—The Office shall be headed by a Director of Domestic Nuclear Detection, who shall be appointed by the President from among individuals nominated by the Secretary.

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

"SEC. 2002. FUNCTIONS OF DIRECTOR OF THE DOMESTIC NUCLEAR DETECTION OFFICE, GENERALLY.

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

"(1) administering all nuclear and radiological detection and prevention functions and assets of the Department, including those functions vested in the Department before the enactment of the Security and Accountability For Every Port Act; and

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

"(b) TRANSFER OF FUNCTIONS.—The Secretary shall transfer to the Director the authority to administer, or supervise the administration of, all functions, personnel, assets, and liabilities of all Department programs and projects relating to nuclear and radiological detection research, development, testing, and evaluation, and nuclear and radiological detection system acquisition and deployment, including with respect to functions and assets transferred by section 303(1)(B), (C), and (E) and functions, assets, and personnel transferred pursuant to section 2010(c).

"SEC. 2003. GLOBAL NUCLEAR DETECTION ARCHITECTURE.

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

"(b) FUNCTIONS OF DIRECTOR.—The Director shall, under subsection (a)—

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

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

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

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

"SEC. 2004. RESEARCH AND DEVELOPMENT.

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

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

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

"(d) COORDINATION WITH OTHER FEDERAL PROGRAMS.—The Director shall coordinate implementation of the program with other Federal agencies performing similar research and development in order to accelerate the development of effective technologies, promote technology sharing, and to avoid duplication, including through the use of the interagency coordination council established under section 2013.

"SEC. 2005. SYSTEM ASSESSMENTS.

"(a) IN GENERAL.—The Director shall carry out a program to test and evaluate technology for detecting nuclear explosive devices and fissile or radiological material.

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

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

"(2) against realistic adversary tactics and countermeasures.

"(c) PROVISION OF TESTING SERVICES.—

"(1) IN GENERAL.—The Director may, under the program, make available testing services to commercial developers of detection devices.

"(2) FEES.—The Director may charge fees, as appropriate, for performance of services under this subsection.

"(d) SYSTEM ASSESSMENTS.—

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

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

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

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

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

"SEC. 2006. TECHNOLOGY ACQUISITION, DEPLOYMENT, SUPPORT, AND TRAINING.

"(a) ACQUISITION STRATEGY.—

"(1) IN GENERAL.—The Director shall develop and, subject to the availability of appropriations, execute a strategy for the acquisition and deployment of detection systems in order to implement the Department components of the global nuclear detection architecture developed under section 2003.

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

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

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

"(c) OPERATIONAL SUPPORT AND PROTOCOLS.—

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

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

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

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

"(e) SOLICITATION OF END-USER INPUT.—In developing requirements for the research and development program of section 2004 and requirements for the acquisition of detection systems to implement the strategy in subsection (a), the Director shall solicit input from end-users of such systems.

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

"SEC. 2007. SITUATIONAL AWARENESS.

"(a) DETECTION INFORMATION.—The Director—

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

"(2) shall gather and archive—

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

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

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

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

"(d) SECURITY.—The Director shall—

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

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

"SEC. 2008. FORENSIC ANALYSIS.

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

"SEC. 2009. THREAT INFORMATION.

"(a) THREAT ASSESSMENTS.—The Director shall utilize classified and unclassified nuclear and radiological threat assessments in designing the global nuclear detection architecture under section 2003, prioritizing detection system deployments, and testing and optimizing system performance of that architecture, including assessments of—

"(1) smuggling routes;

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

"(3) relevant terrorist tradecraft and concealment methods;

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

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

"(c) ANALYTICAL SUPPORT.—The Director shall request that the Secretary provide to the Director, pursuant to section 201(d)(18), the requisite intelligence and information analysis support necessary to effectively discharge the Director's responsibilities.

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

"(e) COLLECTION REQUESTS.—The Director shall recommend to the Secretary consultation that should occur pursuant to section 201(d)(10) regarding intelligence collection to design, deploy, and support the operation of the global detection architecture under section 2003.

"SEC. 2010. ADMINISTRATIVE AUTHORITIES.

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

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

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

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

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

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

"SEC. 2011. REPORT REQUIREMENT.

"The Director shall submit to the appropriate congressional committees an annual report on the following:

"(1) The global detection strategy developed under section 2003.

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

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

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

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

"SEC. 2012. ADVISORY COUNCIL ON NUCLEAR DETECTION.

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

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

"(1) advise the Director on recommendations for the global nuclear detection architecture developed under section 2003(a);

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

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

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

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

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

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

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

"SEC. 2013. INTERAGENCY COORDINATION COUNCIL.

"The President—

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

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

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

"SEC. 2014. AUTHORIZATION OF APPROPRIATIONS.

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

"(1) $536,000,000 for fiscal year 2007; and

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

"SEC. 2015. DEFINITIONS.

"In this title:

"(1) The term 'Director' means the Director of the Domestic Nuclear Detection Office.

"(2) The term 'fissile materials' means materials capable of sustaining a nuclear chain reaction.

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

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

"(5) The term 'Office' means the Domestic Nuclear Detection Office.

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

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

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

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

(b) CONFORMING AMENDMENTS.—

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

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

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

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

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

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

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

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

"TITLE XX—OFFICE OF DOMESTIC NUCLEAR DETECTION

"Sec. 2001. Domestic Nuclear Detection Office.
"Sec. 2002. Functions of Director of the Domestic Nuclear Detection Office, generally.
"Sec. 2003. Global nuclear detection architecture.
"Sec. 2004. Research and development.
"Sec. 2005. System assessments.
"Sec. 2006. Technology acquisition, deployment, support, and training.
"Sec. 2007. Situational awareness.
"Sec. 2008. Forensic analysis.
"Sec. 2009. Threat information.
"Sec. 2010. Administrative authorities.
"Sec. 2011. Report requirement.
"Sec. 2012. Advisory Council on Nuclear Detection.
"Sec. 2013. Interagency coordination council.
"Sec. 2014. Authorization of appropriations.
"Sec. 2015. Definitions.".

SEC. 402. NUCLEAR AND RADIOLOGICAL DETECTION SYSTEMS.

(a) DEPLOYMENT.—Not later than September 30, 2007, the Secretary of Homeland Security shall deploy nuclear and radiological detection systems at 22 United States seaports. To the extent feasible, the Secretary shall deploy the next-generation radiation portal monitors tested in the pilot program under subsection (d) at such United States seaports.

(b) STRATEGY.—Not later than 90 days after the date of the enactment of this Act, the Secretary, acting through the Director of the Domestic Nuclear Detection Office of the Department, shall submit to the appropriate congressional committees a strategy for the deployment of nuclear and radiological detection systems at all remaining United States seaports.

(c) CONTENTS.—The strategy submitted under subsection (b) shall include—

(1) a risk-based prioritization of United States seaports at which nuclear and radiological detection systems will deployed;

(2) a proposed timeline of when nuclear and radiological detection systems will be deployed at each of the seaports identified under paragraph (1);

(3) the type of systems to be used at each of the seaports identified under paragraph (1);

(4) standard operating procedures for examining containers with such systems;

(5) the Department policy for using nuclear and radiological detection systems;

(6) a classified annex that details plans for covert testing; and

(7) a classified annex that outlines the risk-based prioritization of seaports used under paragraph (1).

(d) SAFETY PLAN.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees a plan that—

(1) details the health and safety impacts of nuclear and radiological detection systems; and

(2) describes the policy of U.S. Customs and Border Protection for using nuclear and radiological detection systems.

(e) PILOT PROGRAM.—

(1) IN GENERAL.—Not later than January 1, 2007, the Secretary, acting through the Director of the Domestic Nuclear Detection Office of the Department, shall initiate a pilot program to deploy and test the operational perform-

ance of next-generation radiation portal monitors at one or more United States seaports with a high-volume of containerized cargo.

(2) REPORT.—Not later than March 31, 2007, the Secretary shall submit to the appropriate congressional committees a report that contains—

(A) a description of the next-generation radiation portal monitors deployed at United States seaports under the pilot program;

(B) a description of the operational characteristics of the pilot program at selected United States seaports; and

(C) an evaluation of the operational performance of the next-generation radiation portal monitors, including nuisance alarm rates, and a description of the standards used in such evaluation.

(f) DEPLOYMENT OF NEXT-GENERATION RADIATION PORTAL MONITORS.—

(1) IN GENERAL.—If the Secretary, acting through the Director of the Domestic Nuclear Detection Office of the Department, determines that the operational performance of the next-generation radiation portal monitors under the pilot program carried out under subsection (e) has met the standards described subsection (e)(2)(C), the Secretary shall deploy next-generation radiation portal monitors, in fixed or other configurations, at all United States seaports with a high-volume of containerized cargo to improve cargo screening capabilities at such seaports not later than September 30, 2007.

(2) CONGRESSIONAL NOTIFICATION.—If any deployment of next-generation radiation portal monitors is deemed by the Secretary to be operationally infeasible or would result in ineffective, inefficient, or otherwise wasteful use of resources, the Secretary shall notify the appropriate congressional committees and recommend alternative actions.

(g) ENHANCING OVERSEAS DETECTION CAPABILITIES.—The Secretary, acting through the Director of the Domestic Nuclear Detection Office of the Department, shall work with appropriate Federal departments and agencies to coordinate the installation of nuclear and radiological detection systems at foreign seaports.

(h) DEFINITIONS.—In this section:

(1) NEXT-GENERATION RADIATION PORTAL MONITORS.—The term "next-generation radiation portal monitors" means non-intrusive, containerized cargo examination technologies that possess radionuclide isotope identification capabilities.

(2) NUCLEAR AND RADIOLOGICAL DETECTION SYSTEM.—The term "nuclear and radiological detection system" means any technology that is capable of detecting or identifying nuclear and radiological material or explosive devices.

PURPOSE AND SUMMARY

The purpose of H.R. 4954 is to improve maritime and cargo security through enhanced layered defenses, and for other purposes.

BACKGROUND AND NEED FOR LEGISLATION

Maritime vessels are the primary mode of transportation for international trade, carrying over 80 percent of international trade by volume. In 2004, the United States imported approximately $1.47 trillion in goods, with $423 billion in goods arriving via container ships. Approximately 9,700,000 containers carried these goods into our seaports where they were redirected throughout the nation. United States trade is global in nature, and requires an international, layered, and risk-based security approach.

In its final report, the National Commission on Terrorist Attacks Upon the United States noted, "While commercial aviation remains a possible target, terrorists may turn their attention to other modes of transportation. Opportunities to do harm are as great, or greater in maritime or surface transportation." In May 2002, the Brookings Institution estimated that costs associated with United States port closures from a detonated terrorist weapon could cost the U.S. economy $1 trillion and dramatically affect our trade policies. In March 2006, the Congressional Budget Office determined the cost of shutting down America's largest container port, Los Angeles and

Long Beach, for three years would cost the U.S. economy one million jobs.

Since the terrorist attacks of September 11, 2001, the Federal Government has taken several significant steps to improve our maritime and homeland security, but none have improved comprehensive international supply chain and cargo security provisions. On November 25, 2002, the President signed into law the Maritime Transportation Security Act of 2002 (P.L. 107–295) to improve domestic port security by requiring the completion of detailed vessel and facility security plans, the development of a common transportation worker identification card, the training of specialized Maritime Safety and Security Teams to thwart terrorist activities within the port regions, and other purposes. That same day, the President signed the Homeland Security Act of 2002 (P.L. 107–296), combining twenty-two separate agencies or portions of agencies and establishing the Department of Homeland Security.

A series of hearings, site visits, and oversight work by the Committee on Homeland Security led to the conclusion that the Department of Homeland Security must improve the global supply chain and take additional steps to protect our ports. While the Committee applauds the Department's efforts to take independent action by developing the Container Security Initiative and Customs-Trade Partnership Against Terrorism programs, it seeks to codify these programs and provide guidance to their future operations. The Committee also used this legislation to provide the Department the necessary authorities to acquire additional data necessary for assessing risk of specific cargo shipments, to expand existing maritime security command centers, and institute a new, risk-based Port Security Grant Program to replace that outlined in the Maritime Transportation Security Act. Additionally, the Committee is concerned about the proliferation of weapons of mass destruction and related materials, and created the Domestic Nuclear Detection Office to coordinate the domestic detection efforts to counter these high-consequence threats.

HEARINGS AND BRIEFINGS

On Tuesday, March 22, 2005, the Committee held a field hearing in Vicksburg, Mississippi, entitled "Protecting Our Commerce: Port and Waterways Security." The Committee received testimony from RADM Robert Duncan, Commander Eighth Coast Guard District, United States Coast Guard; Mr. Jimmy Heidel, Executive Director, Warren County Port Commission and Vice-President of the Vicksburg-Warren County Chamber of Commerce; Ms. Cynthia Swain, Director of Safety and Security, Port of New Orleans; Dr. Deirdre McGowan, Executive Director, Inland Rivers, Ports and Terminals Association.

On April 19 and 20, 2005, the Subcommittee on Prevention of Nuclear and Biological Attack held a hearing entitled "DHS Coordination of Nuclear Detection Efforts." On Tuesday, April 19, 2005, the Subcommittee received testimony from Dr. Graham Allison, Director of the Belfer Center for Science and International Affairs, Harvard University; Dr. Fred Iklé, Center for Strategic and International Studies; and Col. Randy Larsen (Ret. USAF), Chief Executive Officer, Homeland Security Associates, LLC. On Wednesday, April 20, 2005, the Subcommittee received testimony from Mr. Vayl

Oxford, Acting Director, Domestic Nuclear Detection Office, Department of Homeland Security.

On Wednesday, June 8, 2005, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity held a hearing entitled "The Homeland Security Missions of the Post-9/11 Coast Guard." Testimony was received from Admiral Thomas Collins, Commandant United States Coast Guard, Department of Homeland Security.

On June 21, 2005, the Subcommittee on Prevention of Nuclear and Biological Attack and the Subcommittee on Emergency Preparedness, Science, and Technology held a joint hearing entitled "Detecting Nuclear Weapons and Radiological Materials: How Effective Is Available Technology?" The Subcommittee received testimony from Mr. Gene Aloise, Director, Natural Resources and Environment, Government Accountability Office; Dr. Richard L. Wagner, Jr., Chair, Defense Science Board Task Force on Prevention of, and Defense Against, Clandestine Nuclear Attack and Senior Staff Member, Los Alamos National Laboratory; Ms. Bethann Rooney, Manager, Port Security, Port Authority of New York & New Jersey; Dr. Benn Tannenbaum, American Association for the Advancement of Science; Mr. Vayl Oxford, Acting Director, Domestic Nuclear Detection Office, Department of Homeland Security; Mr. Michael K. Evenson, Acting Director, Combat Support Directorate, DTRA, Department of Defense; and Mr. David Huizenga, Assistant Deputy Administrator, International Materials Protection and Cooperation, National Nuclear Security Administration, Department of Energy.

On June 28, 2005, the Subcommittee on Prevention of Nuclear and Biological Attack held a hearing, "Pathways to the Bomb: Security of Fissile Materials Abroad." The Subcommittee received testimony from Mr. David Albright, Director, Institute for Science and International Security; and Ms. Rose Gottemoeller, Senior Associate, Carnegie Endowment for International Peace. On the same date, the Subcommittee also received a classified briefing on the same issue from representatives from the Administration.

On July 21, 2005, the Subcommittee on Prevention of Nuclear and Biological Attack held a classified briefing on the new Domestic Nuclear Detection Office, and the development and testing of nuclear detection technology.

On September 22, 2005, the Subcommittee on Prevention of Nuclear and Biological Attack held a hearing entitled "Trends in Illicit Movement of Nuclear Materials." The Subcommittee received testimony from Dr. Rensselaer Lee, President, Global Advisory Services; Dr. Raymond J. Juzaitis, Associate Director, Nonproliferation, Arms Control, and International Security, Lawrence Livermore National Laboratory, University of California; and Mr. Glenn E. Schweitzer, Director for Central Europe and Eurasia, The National Academy of Sciences.

January 23 and 24, 2006, the Members of the Subcommittee on Prevention of Nuclear and Biological Attack conducted a site visit of the Department of Homeland Security's Radiological/Nuclear Countermeasures Test and Evaluation Complex (Rad/NucCTEC) at the Nevada Test Site, Las Vegas, Nevada. The tour of the facility included a discussion and analysis of hand-held radiation detectors and the development of portal monitors.

On February 15, 2006, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity held a hearing entitled "The President's Fiscal Year 2007 Budget: Coast Guard Programs Impacting Maritime Border Security." The Subcommittee received testimony from Admiral Thomas H. Collins, Commandant, U.S. Coast Guard.

On June 22, 2005, the Members of the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment received a closed Member briefing on Assessing the Threat to America's Ports. Representatives from the United States Coast Guard, and the Office of Information Analysis both of the Department of Homeland Security.

On March 1, 2006, the Members of the Committee on Homeland Security and the Members of the Permanent Select Committee on Intelligence received a classified briefing on the intelligence analysis included in the Committee on Financial Investment in the United States (CFIUS) 30-day review of the Dubai Ports World (DP World) proposed acquisition of Peninsular & Oriental Steam Navigation Co. (P&O). Representatives from the Department of Treasury; the Department of Homeland Security; the Office of the Director of National Intelligence; and the Defense Intelligence Agency were present.

On March 16, 2006, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity held a hearing on H.R. 4954. Testimony was received from Mr. Jayson Ahern, Assistant Commissioner, Office of Field Operations, Customs and Border Protection, Department of Homeland Security; Captain Brian Salerno, Deputy Director, Inspections & Compliance, United States Coast Guard, Department of Homeland Security; Mr. Eugene Pentimonti, Senior Vice President, Government Relations, MAERSK Inc.; and Mr. Noel Cunningham, Principal, MARSEC Group.

On March 17, 2006, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity conducted a site visit at the Ports of Los Angeles and Long Beach. The site visit included a roundtable discussion with port security experts and operational entities, as well as a tour of the facilities.

On April 4, 2006, the Full Committee held a hearing on H.R. 4954. The Committee received testimony from the Honorable Michael P. Jackson, Deputy Secretary, Department of Homeland Security; Ms. Bethann Rooney, Manager of Port Security, Port Authority of New York and New Jersey; Mr. Christopher L. Koch, President and CEO, World Shipping Council; Mr. Jonathan E. Gold, Vice President, Global Supply Chair Policy, Retail Industry Leaders Association; and Mr. Clark Kent Ervin, private citizen.

On April 19, 2006, Staff of the Subcommittee on Prevention of Nuclear and Biological Attack conducted a site visit of the Edgewater Chemical Biological Center at the Aberdeen Proving Ground, Aberdeen, Maryland. Subcommittee staff toured the facility and examined a mobile laboratory.

On April 20, 2006, staff of the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment received a briefing from the Customs and Border Protection, Office of Intelligence, to observe how Customs and Border Protection collects information at the points of Entry.

COMMITTEE CONSIDERATION

H.R. 4954 was introduced by Mr. Lungren and 45 original cosponsors on March 14, 2006, and referred solely to the Committee on Homeland Security. Within the Committee, H.R. 4954 was referred to the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity on March 15, 2006.

On March 16, 2006, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity held a hearing on H.R. 4954. Testimony was received from Mr. Jayson Ahern, Assistant Commissioner, Office of Field Operations, Customs and Border Protection, Department of Homeland Security; Captain Brian Salerno, Deputy Director, Inspections & Compliance, United States Coast Guard, Department of Homeland Security; Mr. Eugene Pentimonti, Senior Vice President, Government Relations, MAERSK Inc.; and Mr. Noel Cunningham, Principal, MARSEC Group.

On March 30, 2006, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity met in open markup session, a quorum being present, and ordered H.R. 4954 favorably forwarded to the Full Committee, as amended, by voice vote.

On April 4, 2006, the Full Committee held a hearing on H.R. 4954. The Committee received testimony from the Honorable Michael P. Jackson, Deputy Secretary, Department of Homeland Security; Ms. Bethann Rooney, Manager of Port Security, Port Authority of New York and New Jersey; Mr. Christopher L. Koch, President and CEO, World Shipping Council; Mr. Jonathan E. Gold, Vice President, Global Supply Chair Policy, Retail Industry Leaders Association; and Mr. Clark Kent Ervin, private citizen.

On April 26, 2006, the Full Committee met in open markup session and ordered H.R. 4954 favorably reported to the House of Representatives, as 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 April 26, 2006, the Full Committee considered H.R. 4954, to improve maritime and cargo security through enhanced layered defenses, and for other purposes, and ordered the bill favorably reported to the House, amended, by voice vote. H.R. 4954 was AGREED TO, as amended, by a recorded vote of 29 yeas and 0 nays (Roll Call Vote No. 34). The vote was as follows:

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

Date: Wednesday, April 26, 2006 Convened: 10:11 a.m.

Adjourned: 3:35 p.m.

Meeting on : Markup of H.R. 4954, to improve maritime and cargo security through enhanced layered defenses, and for other purposes. On agreeing to H.R. 4954, as amended.

☐ Attendance ☒ Recorded Vote Vote Number: 34 Total: Yeas 29 Nays 0

	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	**29**	**0**	

The following amendments were offered:

An Amendment in the Nature of a Substitute (#1) offered by Mr. King; was AGREED TO, amended, by voice vote. A unanimous consent request by Mr. King to consider the Amendment in the Nature of a Substitute as base text for purposes of amendment, was objected to.

An amendment offered by Mr. Thompson to the Amendment in the Nature of a Substitute (#1A); in section 103, redesignate subsection (f) as subsection (g) and insert after subsection (e) the following new subsection entitled "(f) Appeals Process for More Stringent State Standards."; was WITHDRAWN by unanimous consent.

An amendment offered by Ms. Jackson-Lee to the Amendment in the Nature of a Substitute (#1B); in section 510(d)(4) of the Homeland Security Act of 2002 (as proposed to be added by section 105 of the amendment), strike all after "Area Maritime Security Plan" and insert a semicolon.; was NOT AGREED TO by recorded vote of 12 yeas and 18 nays (Roll Call Vote No. 25). The vote was as follows:

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

Date: Wednesday, April 26, 2006 Convened: 10:11 a.m.

Adjourned: 3:35 p.m.

Meeting on : Markup of H.R. 4954, to improve maritime and cargo security through enhanced layered defenses, and for other purposes. Amendment #1B offered by Ms. Jackson-Lee.

☐ Attendance ☒ Recorded Vote Vote Number: 25 Total: Yeas 12 Nays 18

	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	**12**	**18**	

An amendment offered by Mr. Thompson to the Amendment in the Nature of a Substitute (#1C); page 30, after line 5, insert the following new section entitled "Sec. 113. Additional Customs and Border Protection Officers at United States Seaports."; was NOT AGREED TO by a recorded vote of 13 yeas and 17 nays (Roll Call Vote No. 26). The vote was as follows:

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

Date: Wednesday, April 26, 2006 Convened: 10:11 a.m.

Adjourned: 3:35 p.m.

Meeting on : Markup of H.R. 4954, to improve maritime and cargo security through enhanced layered defenses, and for other purposes. Amendment #1C offered by Mr. Thompson.

☐ Attendance ☒ Recorded Vote Vote Number: 26 Total: Yeas 13 Nays 17

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska		✓		*Mr. Bennie G. Thompson* *Mississippi, Ranking Member*	✓		
Mr. Lamar S. Smith Texas		✓		*Ms. Loretta Sanchez* *California*	✓		
Mr. Curt Weldon Pennsylvania				*Mr. Edward J. Markey* *Massachusetts*	✓		
Mr. Christopher Shays Connecticut		✓		*Mr. Norman D. Dicks* *Washington*	✓		
Mr. John Linder Georgia		✓		*Ms. Jane Harman* *California*	✓		
Mr. Mark E. Souder Indiana		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Tom Davis Virginia		✓		*Ms. Nita M. Lowey* *New York*			
Mr. Daniel E. Lungren California		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*	✓		
Mr. Jim Gibbons Nevada		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Rob Simmons Connecticut		✓		*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Mike Rogers Alabama		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*	✓		
Ms. Katherine Harris Florida				*Mr. Bob Etheridge* *North Carolina*	✓		
Mr. Bobby Jindal Louisiana		✓		*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Dave Reichert Washington		✓		*Mr. Kendrick Meek* *Florida*	✓		
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Ms. Ginny Brown-Waite Florida		✓					
Mr. Peter T. King New York Chairman		✓		Total	**13**	**17**	

An amendment offered by Mrs. Christensen, to the Amendment in the Nature of a Substitute (#1D); page 30, after line 5, insert the following new section entitled "Sec. _____. Border Patrol Unit for Virgin Islands."; was AGREED TO by voice vote.

An amendment offered by Mr. Reichert to the Amendment in the Nature of a Substitute (#1E); at the end of title I, insert the following new section entitled "Sec. 111. Port Security Exercise Program."; was AGREED TO by voice vote.

An amendment offered by Mr. Reichert to the Amendment in the Nature of a Substitute (#1F); at the end of title I, insert the following new section entitled "Sec. 111. Port Security Training Program."; was AGREED TO by voice vote.

An amendment offered by Ms. Sanchez to the Amendment in the Nature of a Substitute (#1G); page 49, line 24, add at the end the following new sentence: "Such benefits may not include reduced scores in the Automated Targeting System."; was NOT AGREED TO by a recorded vote of 11 yeas and 17 nays (Roll Call Vote No. 24). The vote was as follows:

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

Date: Wednesday, April 26, 2006 Convened: 10:11 a.m.

Adjourned: 3:35 p.m.

Meeting on : Markup of H.R. 4954, to improve maritime and cargo security through enhanced layered defenses, and for other purposes. Amendment #1G offered by Ms. Sanchez.

☐ Attendance ☒ Recorded Vote Vote Number: 24 Total: Yeas 11 Nays 17

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska		✓		*Mr. Bennie G. Thompson* *Mississippi, Ranking Member*	✓		
Mr. Lamar S. Smith Texas		✓		*Ms. Loretta Sanchez* *California*	✓		
Mr. Curt Weldon Pennsylvania				*Mr. Edward J. Markey* *Massachusetts*	✓		
Mr. Christopher Shays Connecticut		✓		*Mr. Norman D. Dicks* *Washington*	✓		
Mr. John Linder Georgia		✓		*Ms. Jane Harman* *California*	✓		
Mr. Mark E. Souder Indiana		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Tom Davis Virginia		✓		*Ms. Nita M. Lowey* *New York*			
Mr. Daniel E. Lungren California		✓		*Ms. Eleanor Holmes Norton* *District of Columbia*	✓		
Mr. Jim Gibbons Nevada		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Rob Simmons Connecticut		✓		*Ms. Sheila Jackson-Lee* *Texas*			
Mr. Mike Rogers Alabama		✓		*Mr. Bill Pascrell, Jr.* *New Jersey*	✓		
Mr. Stevan Pearce New Mexico		✓		*Mrs. Donna M. Christensen* *U.S. Virgin Islands*			
Ms. Katherine Harris Florida				*Mr. Bob Etheridge* *North Carolina*	✓		
Mr. Bobby Jindal Louisiana		✓		*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Dave Reichert Washington		✓		*Mr. Kendrick Meek* *Florida*			
Mr. Michael McCaul Texas		✓					
Mr. Charlie Dent Pennsylvania		✓					
Ms. Ginny Brown-Waite Florida		✓					
Mr. Peter T. King New York Chairman		✓		Total	**11**	**17**	

An amendment offered by Ms. Brown-Waite to the Amendment in the Nature of a Substitute (#1H); at the appropriate place in the amendment, insert the following new section entitled "Sec._____ Next Generation Supply Chain Security Technologies."; was AGREED TO by a recorded vote of 33 yeas and 0 nays (Roll Call Vote No. 27). The vote was as follows:

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

Date: Wednesday, April 26, 2006 Convened: 10:11 a.m.

Adjourned: 3:35 p.m.

Meeting on : Markup of H.R. 4954, to improve maritime and cargo security through enhanced layered defenses, and for other purposes. Amendment #1H offered by Ms. Brown-Waite.

☐ Attendance ☒ Recorded Vote Vote Number: 27 Total: Yeas 33 Nays 0

	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	**33**	**0**	

An amendment offered by Mr. Markey to the Amendment in the Nature of a Substitute (#1I); to strike section 1804 as proposed by section 201; and insert a new section 202 entitled "Sec. 202. Requirements Relating to Entry of Containers Into the United States."; was NOT AGREED TO by a recorded vote of 16 yeas and 18 nays (Roll Call Vote No. 28). The vote was as follows:

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

Date: Wednesday, April 26, 2006 Convened: _____

Adjourned: _____

Meeting on : Markup of H.R. 4954, to improve maritime and cargo security through enhanced layered defenses, and for other purposes. Amendment # 1I offered by Mr. Markey

☐ Attendance ☒ Recorded Vote Vote Number: 28 Total: Yeas 16 Nays 18

	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	16	18	

An amendment offered by Ms. Jackson-Lee to the Amendment in the Nature of a Substitute (#1J); at the end of title I, insert the following new section entitled "Sec. _____. Study and Report by Comptroller General."; was NOT AGREED TO by a recorded vote of 11 yeas and 13 nays (Roll Call Vote No. 29). The vote was as follows:

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

Date: Wednesday, April 26, 2006 Convened: _____

Adjourned: _____

Meeting on : Markup of H.R. 4954, to improve maritime and cargo security through enhanced layered defenses, and for other purposes. Amendment # 1J offered by Ms. Jackson-Lee

☐ Attendance ☒ Recorded Vote Vote Number: 29 Total: Yeas 11 Nays 13

	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	11	13	

An amendment offered by Ms. Jackson-Lee to the Amendment in the Nature of a Substitute (#1K); at the end of title I, insert the following new section entitled "Sec. _____. Study and Report by Secretary of Homeland Security."; was AGREED TO by voice vote.

An amendment offered by Ms. Jackson-Lee to the Amendment in the Nature of a Substitute (#1L); at the end of title I, insert the following new section entitled "Sec. _____ Moratorium on Certain Contracts to Conduct Port Operations In the United States."; was NOT AGREED TO by a recorded vote of 11 yeas and 13 nays (Roll Call Vote No. 30). The vote was as follows:

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

Date: Wednesday, April 26, 2006 Convened: _____

Adjourned: _____

Meeting on : Markup of H.R. 4954, to improve maritime and cargo security through enhanced layered defenses, and for other purposes. Amendment # 1L offered by Ms. Jackson-Lee

☐ Attendance ☒ Recorded Vote Vote Number: 30 Total: Yeas 11 Nays 13

	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	11	13	

An amendment offered by Ms. Jackson-Lee to the Amendment in the Nature of a Substitute (#1M); page 73, line 8, strike "The head" and insert the following new subsections "(1) In General."; and "(2) Qualifications."; was AGREED TO, as modified, by voice vote. A unanimous consent request by Ms. Jackson-Lee to modify her amendment by striking on line 7 ", international relations, and business management"; was not objected to.

An amendment offered by Mr. Langevin to the Amendment in the Nature of a Substitute (#1N); in section 2006(a) of the Homeland Security Act of 2002 (as proposed to be added by section 401 of the amendment), add at the end the following new paragraphs entitled "(4) Additional Requirements."; "(5) Report" and in section 2014(1) of the Homeland Security Act of 2002 (as proposed to be added by section 401 of the amendment), strike "$536,000,000" and insert "$653,000,000"."; was NOT AGREED TO by a recorded vote of 10 yeas and 14 nays (Roll Call Vote No. 31). The vote was as follows:

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

Date: Wednesday, April 26, 2006 Convened: _____

Adjourned: _____

Meeting on : Markup of H.R. 4954, to improve maritime and cargo security through enhanced layered defenses, and for other purposes. Amendment # 1N offered by Mr. Langevin

☐ Attendance ☒ Recorded Vote Vote Number: 31 Total: Yeas 10 Nays 14

	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	10	14	

An amendment offered by Mr. Langevin to the Amendment in the Nature of a Substitute (#1O); In section 2014(1) of the Homeland Security Act of 2002 (as proposed to be added by section 401 of the amendment), strike "$536,000,000" and insert "$1,836,000,000".; was NOT AGREED TO by a recorded vote of 10 yeas and 15 nays (Roll Call Vote No. 32). The vote was as follows:

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

Date: Wednesday, April 26, 2006 Convened: _____

Adjourned: _____

Meeting on : Markup of H.R. 4954, to improve maritime and cargo security through enhanced layered defenses, and for other purposes. Amendment # 1O offered by Mr. Langevin

☐ Attendance ☒ Recorded Vote Vote Number: 32 Total: Yeas 10 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	10	15	

An amendment offered by Mr. Thompson to the Amendment in the Nature of a Substitute (#1P); add the end the following new section entitled "Sec. ____. Reserve Officers and Junior Reserve Officers Training Pilot Project."; was AGREED TO by voice vote.

An amendment offered by Ms. Jackson-Lee to the Amendment in the Nature of a Substitute (#1Q); page 80, line 21, strike "The Office" and insert the following "(1) In General.—The Office"; and on page 81, after line 2, insert a new paragraph (2) entitled "Qualifications."; was NOT AGREED TO by a recorded vote of 11 yeas and 15 nays (Roll Call Vote No. 33). The vote was as follows:

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

Date: Wednesday, April 26, 2006 Convened: _____

Adjourned: _____

Meeting on : Markup of H.R. 4954, to improve maritime and cargo security through enhanced layered defenses, and for other purposes. Amendment # 1Q offered by Ms. Jackson-Lee

☐ Attendance ☒ Recorded Vote Vote Number: 33 Total: Yeas 11 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	11	15	

An amendment offered by Mrs. Christensen to the Amendment in the Nature of a Substitute (#1R); add at the end the following new section entitled "Sec. _____. Acceleration of Integrated Deepwater Program."; was AGREED TO by voice vote

An amendment offered by Mrs. Christensen to the Amendment in the Nature of a Substitute (#1S); at the appropriate place in the bill, insert the following new section entitled "Sec. _____ Study Relating to Impact of Providing Arrival and Departure Manifests for Certain Commercial Vessels in the United States Virgin Islands."; was AGREED TO by voice vote.

An amendment offered by Ms. Harris to the Amendment in the Nature of a Substitute (#1T); page 26, line 21, strike "overtime" and insert "expenses".; was AGREED TO by voice vote.

On March 30, 2006, the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity considered H.R. 4954, to improve maritime and cargo security through enhanced layered defenses, and for other purposes; and ordered the bill favorably forwarded to the Full Committee for consideration, amended, by voice vote.

The following amendments were offered:

An Amendment in the Nature of a Substitute (#1) offered by Mr. Lungren; was AGREED TO, amended, by voice vote.

An amendment offered by Ms. Sanchez to the Amendment in the Nature of a Substitute (#1A), after section 7, insert the following new section entitled "Review of Waiver Denial; Additional Waiver Request."; was WITHDRAWN by unanimous consent.

An amendment offered by Ms. Sanchez to the Amendment in the Nature of a Substitute (#1B), on page 22, after line 13, insert the following new subsection "(d) Pilot Program."; was AGREED TO by voice vote.

An amendment offered by Ms. Sanchez to the Amendment in the Nature of a Substitute (#1C), on page 29, line 14, add at the end the following new sentence: "Such benefits may not include reduced scores in the Automated Targeting System."; was NOT AGREED TO by a recorded vote of 5 yeas and 6 nays (Roll Call Vote No. 3). The vote was as follows:

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

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

Date: Thursday, March 30, 2006 Convened: 10:05 a.m.

Adjourned: 12:34 p.m.

Meeting on : Markup of H.R. 4954, SAFE Port Act – Amendment #1C offered by Ms. Sanchez

☐ Attendance ☒ Recorded Vote Vote Number: 3 Total: Yeas 5 Nays 6

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska				*Ms. Loretta Sanchez* *California*	✓		
Mr. Lamar S. Smith Texas		✓		*Mr. Edward J. Markey* *Massachusetts*	✓		
Mr. John Linder Georgia		✓		*Mr. Norman D. Dicks* *Washington*			
Mr. Mark E. Souder Indiana		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Mike Rogers Alabama		✓		*Ms. Zoe Lofgren* *California*			
Mr. Stevan Pearce New Mexico				*Ms. Sheila Jackson-Lee* *Texas*			
Ms. Katherine Harris Florida				*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Bobby Jindal Louisiana							
				Mr. Bennie G. Thompson *Mississippi, (Ex Officio)*	✓		
Mr. Peter T. King New York, (Ex Officio)		✓					
Mr. Daniel E. Lungren California, Chairman		✓					
				Total	5	6	

An amendment offered by Mr. Markey to the Amendment in the Nature of a Substitute (#1D), on page 21, strike line 7 and all that follows through line 13 on page 22 and insert a new section entitled "Requirements Relating to Entry of Containers Into the United States."; was NOT AGREED TO by a recorded vote of 6 yeas and 8 nays (Roll Call Vote No. 4). The vote was as follows:

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

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

Date: Thursday, March 30, 2006 Convened: 10:05 a.m.
Adjourned: 12:34 p.m.

Meeting on : Markup of H.R. 4954, SAFE Port Act – Amendment #1D offered by Mr. Markey

☐ Attendance ☒ Recorded Vote Vote Number: 4 Total: Yeas 6 Nays 8

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska				*Ms. Loretta Sanchez* *California*	✓		
Mr. Lamar S. Smith Texas				*Mr. Edward J. Markey* *Massachusetts*	✓		
Mr. John Linder Georgia		✓		*Mr. Norman D. Dicks* *Washington*			
Mr. Mark E. Souder Indiana		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Mike Rogers Alabama		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Stevan Pearce New Mexico		✓		*Ms. Sheila Jackson-Lee* *Texas*			
Ms. Katherine Harris Florida		✓		*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Bobby Jindal Louisiana		✓					
				Mr. Bennie G. Thompson *Mississippi, (Ex Officio)*	✓		
Mr. Peter T. King New York, (Ex Officio)		✓					
Mr. Daniel E. Lungren California, Chairman		✓					
				Total	6	8	

An amendment offered by Ms. Sanchez to the Amendment in the Nature of a Substitute (#1E), on page 33, beginning on line 11, strike "If the Secretary utilizes third party entitled to conduct validations of C-TPAT participants" and insert "If the Secretary determined to expand the use of third party entitled to conduct validation of C-TPAT Participants upon completion of the pilot program under paragraph (6).."; was AGREED TO by voice vote.

An amendment offered by Ms. Sanchez to the Amendment in the Nature of a Substitute (#1F), on page 38, line 20, strike "3-year period" and insert "2-year period."; was NOT AGREED to by voice vote.

An amendment offered by Mr. Thompson to the Amendment in the Nature of a Substitute (#1G), on page 78, before line 1, insert the following new section entitled "Additional Customs and Border Protection Officers at United States Seaports."; was NOT AGREED TO by a recorded vote of 6 yeas and 7 nays (Roll Call Vote No. 5). The vote was as follows:

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

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

Date: Thursday, March 30, 2006 Convened: 10:05 a.m.

Adjourned: 12:34 p.m.

Meeting on : Markup of H.R. 4954, SAFE Port Act – Amendment #1G offered by Mr. Thompson

☐ Attendance ☒ Recorded Vote Vote Number: 5 Total: Yeas 6 Nays 7

	YEA	NAY	PRESENT		YEA	NAY	PRESENT
Mr. Don Young Alaska				*Ms. Loretta Sanchez* *California*	✓		
Mr. Lamar S. Smith Texas				*Mr. Edward J. Markey* *Massachusetts*	✓		
Mr. John Linder Georgia		✓		*Mr. Norman D. Dicks* *Washington*			
Mr. Mark E. Souder Indiana		✓		*Mr. Peter A. DeFazio* *Oregon*	✓		
Mr. Mike Rogers Alabama		✓		*Ms. Zoe Lofgren* *California*	✓		
Mr. Stevan Pearce New Mexico				*Ms. Sheila Jackson-Lee* *Texas*			
Ms. Katherine Harris Florida		✓		*Mr. James R. Langevin* *Rhode Island*	✓		
Mr. Bobby Jindal Louisiana		✓					
				Mr. Bennie G. Thompson *Mississippi, (Ex Officio)*	✓		
Mr. Peter T. King New York, (Ex Officio)		✓					
Mr. Daniel E. Lungren California, Chairman		✓					
				Total	6	7	

An amendment offered by Mr. Thompson to the Amendment in the Nature of a Substitute (#1H), At the appropriate place in the bill, insert the following new section entitled "Transfer of Megaports Program to the Department of Homeland Security."; was WITHDRAWN by unanimous consent.

An amendment offered by Mr. Linder to the Amendment in the Nature of a Substitute (#1I), on page 24, line 6, insert new subsections entitled "(C) Pilot Program."; "(d) Deployment of Next-Generation Radiation Portal Monitors."; and redesignate section (c) as (e); was AGREED TO by voice vote.

An amendment offered by Mr. Langevin to the Amendment in the Nature of a Substitute (#1J), at the appropriate place in the bill, insert the following new sections entitled "Amendment to the Defense Production Act of 1950."; and "Sense of Congress."; was WITHDRAWN by unanimous consent.

An amendment offered by Mr. Jindal to the Amendment in the Nature of a Substitute (#1K), at the appropriate place in the bill, to insert a new section entitled "Information Sharing."; was AGREED TO by voice vote.

COMMITTEE OVERSIGHT FINDINGS

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

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

The purpose of H.R. 4954, the "Security and Accountability For Every Port Act" or "SAFE Port Act", is to improve maritime and cargo security through enhanced layered defenses.

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. 4954, the SAFE Port Act, 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, April 28, 2006.

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

DEAR MR. CHAIRMAN: The Congressional Budget Office has completed the enclosed cost estimate for H.R. 4954, the Security and Accountability For Every Port Act.

The CBO staff contacts for this estimate are Mark Grabowicz (for federal costs), who can be reached at 226–2860, Sarah Puro (for the impact on state and local governments), who can be reached at

225–3220, and Paige Piper/Bach (for the impact on the private sector), who can be reached at 226–2940.

Sincerely,

DONALD B. MARRON,
Acting Director.

Enclosure.

H.R. 4954—Security and Accountability for Every Port Act

Summary: CBO estimates that H.R. 4954 would authorize the appropriation of $8.9 billion over the 2007–2011 period for Department of Homeland Security (DHS) programs to improve the security of U.S. ports, for the Domestic Nuclear Detection Office within DHS, and for the United States Coast Guard's integrated deepwater program (IDP). In addition, the bill would specifically authorize the appropriation of an additional $881 million in 2012 for port security programs. Assuming appropriation of the necessary amounts, CBO estimates that implementing H.R. 4954 would cost $7.4 billion over the 2007–2011 period and additional spending of more than $2 billion after 2011. Enacting the bill could affect direct spending and receipts, but we estimate that any such effects would not be significant.

H.R. 4954 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that the costs to intergovernmental entities, including public ports, would total less than $10 million annually, and would not exceed the threshold established in UMRA ($64 million in 2006, adjusted for inflation).

H.R. 4954 would impose new private-sector mandates, as defined in UMRA, on owners and operators of maritime terminal facilities. CBO estimates that the direct cost of complying with those mandates would be small and would fall below the annual threshold for private-sector mandates ($128 million in 2006, adjusted annually for inflation). In addition, the bill would require the Secretary of DHS to review and issue certain regulations. Because those regulations have not been established, CBO cannot determine if additional mandates would be imposed. Therefore, CBO cannot determine whether the aggregate direct cost of complying with all of the private-sector mandates that may be imposed by the bill would exceed the annual threshold.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 4954 is shown in the following table. The costs of this legislation fall within budget functions 400 (transportation), 450 (community and regional development), and 750 (administration of justice).

	By fiscal year, in millions of dollars—					
	2006	2007	2008	2009	2010	2011
SPENDING SUBJECT TO APPROPRIATION						
Spending Under Current Law for Programs:						
Authorized by H.R. 4954						
Budget Authority[1]	1,441	0	0	0	0	0
Estimated Outlays	769	534	363	150	70	40
Proposed Changes:						
DHS Programs to Improve Port Security:						
Authorization Level	0	801	801	821	841	861
Estimated Outlays	0	307	520	724	835	855

	By fiscal year, in millions of dollars					
	2006	2007	2008	2009	2010	2011
Domestic Nuclear Detection Office:						
Estimated Authorization Level	0	536	552	569	586	603
Estimated Outlays	0	268	437	557	574	591
Integrated Deepwater Program:						
Authorization Level	0	1,892	0	0	0	0
Estimated Outlays	0	189	530	530	284	151
Other DHS Programs:						
Estimated Authorization Level	0	4	2	2	2	2
Estimated Outlays	0	3	2	2	2	2
Total Changes:						
Estimated Authorization Level	0	3,233	1,355	1,391	1,428	1,466
Estimated Outlays	0	767	1,488	1,812	1,694	1,599
Spending Under H.R. 4954:						
Estimated Authorization Level [1]	1,441	3,233	1,355	1,391	1,428	1,466
Estimated Outlays	769	1,302	1,851	1,962	1,764	1,639

[1] The 2006 level is the amount appropriated for that year for most programs authorized by H.R. 4954. These programs include the container security initiative, the customs-trade partnership against terrorism, the Domestic Nuclear Detection Office, and the integrated deepwater program. The total does not include any funding for maritime security command centers because this information is not available.

Basis of estimate: For this estimate, CBO assumes that the bill will be enacted before the end of 2006. CBO estimates that implementing H.R. 4954 would cost about $7.4 billion over the 2007–2011 period, assuming appropriation of the authorized and estimated amounts. Enacting the bill could increase both direct spending and receipts, but CBO estimates that any such effects would not be significant in any year.

Spending subject to appropriation

For this estimate, CBO assumes that the amounts authorized or estimated to be necessary will be appropriated for each year. Estimated outlays are based on historical spending patterns for existing or similar programs.

DHS Programs to Improve Port Security. H.R. 4954 would authorize the appropriation of:

- $20 million for fiscal year 2007 for DHS to verify the identity of individuals with access to secure areas of seaports;
- $60 million for each of fiscal years 2007 through 2011 for DHS to establish or expand security command centers at selected seaports;
- $400 million for each of fiscal years 2007 through 2011 for DHS to make grants to improve the security of U.S. ports, especially those at greatest risk;
- $300 million over the 2007–2011 period for DHS to hire new inspection officers at U.S. ports ($20 million for 2007, increasing to $100 million for 2011;
- $5 million for each of fiscal years 2007 through 2011 for DHS to identify high-risk containers moving through international commerce;
- $196 million for each of fiscal years 2007 through 2011 for the container security initiative, a DHS program to examine containers at foreign ports before they are shipped to the United States;
- $75 million for each of fiscal years 2007 through 2011 for DHS to form partnerships with importers and other entities to improve security at U.S. ports; and

- $25 million for each of fiscal years 2007 through 2011 for operation safe commerce, a DHS program that would provide grants to improve cargo inspection at U.S. ports.

Assuming appropriation of the authorized amounts, CBO estimates that implementing these programs would cost about $3.2 billion over the 2007–2011 period.

Domestic Nuclear Detection Office. H.R. 4954 would authorize the appropriation of $536 million for fiscal year 2007 and necessary amounts for each subsequent fiscal year for the Domestic Nuclear Detection Office in DHS. CBO estimated the necessary funding levels in future years by adjusting 2007 funding for anticipated inflation. Thus, implementing this section would cost about $2.4 billion over the 2007–2011 period.

Integrated Deepwater Program. H.R. 4954 would authorize the appropriation of nearly $1.9 billion for fiscal year 2007 for the IDP, the Coast Guard's 25-year, $26 billion program to modernize its aircraft and vessel fleets and improve its command, control, and logistics systems. CBO estimates that implementing this section would cost about $1.7 billion over the 2007–2011 period.

Other Programs. H.R. 4954 would direct DHS to consolidate its port security training programs, establish a border patrol unit for the U.S. Virgin Islands, and carry out pilot programs and reports relating to port security. Based on information from DHS, CBO estimates that it would cost about $10 million over the 2007–2011 period to implement these provisions.

Receipts and direct spending

H.R. 4954 would establish new criminal penalties for the improper use of certain trade data. Thus, the federal government might collect additional fines if the bill is enacted. Collections of criminal fines are deposited in the Crime Victims Fund and later spent. CBO expects that any additional receipts and direct spending would not be significant.

Estimated impact on State, local, and tribal governments: H.R. 4954 contains intergovernmental mandates as defined in UMRA because it would require state and local entities (including law enforcement and port authorities) to participate in staffing command centers for maritime security, resubmit security plans in certain circumstances, and hire a United States citizen for the position of chief security officer. Only the provisions that would require state and local entities to participate in staffing command centers for maritime security would impose significant costs on intergovernmental entities. Based on information from industry and governmental sources, CBO estimates that the costs to intergovernmental entities of these provisions likely would total less than $10 million annually and would not exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

Other provisions of the bill would authorize more than $400 million annually, for fiscal years 2007 through 2012 to improve security and cargo inspection at United States ports. To the extent that state, local, or tribal governments apply for and receive such grants, these provisions would provide benefits to those entities. Any costs resulting from complying with the conditions of the grants would be incurred voluntarily.

Estimated impact on the private sector: H.R. 4954 would impose new private-sector mandates, as defined in UMRA, on owners and operators of maritime terminal facilities. CBO estimates that the direct cost of complying with those mandates would be small and would fall below the annual threshold for private-sector mandates ($128 million in 2006, adjusted annually for inflation). In addition, the bill would require the Secretary of DHS to review and issue certain regulations. Because those regulations have not been established, CBO cannot determine if additional mandates would be imposed. Therefore, CBO cannot determine whether the aggregate direct cost of complying with all of the private-sector mandates that may be imposed by the bill would exceed the annual threshold.

H.R. 4954 would impose mandates on owners and operators of maritime terminal facilities. The bill would require owners and operators of maritime terminal facilities to resubmit their security plans for approval upon transfer of ownership or operation of their facility. The bill also would require that the individual having full authority to implement security actions at a terminal facility be a citizen of the United States. Based on information from industry and government sources, CBO expects that the total direct cost of complying with those requirements would be small relative to UMRA's annual threshold.

The bill also would require the Secretary of DHS to review and promulgate regulations regarding the security of the international supply chain. Those regulations could impose new mandates on shipping carriers and owners and operators of maritime terminal facilities. The provisions would require the Secretary to issue rules on:

- The transmission of certain data to DHS prior to the loading of cargo for shipment to the United States;
- Minimum standards and verification procedures for securing and sealing containers in transit to the United States; and
- The identification of high-risk containers in the international supply chain.

Because those regulations have not been established, CBO cannot determine if such regulations would impose new mandates on the private sector.

Previous CBO Estimate: On March 29, 2006, CBO transmitted a cost estimate for S. 1052, the Transportation Security Improvement Act of 2005, as reported by the Senate Committee on Commerce, Science, and Transportation on February 27, 2006. CBO estimated that implementing S. 1052 would cost over $3 billion in 2007 and nearly $12 billion over the 2007–2011 period, assuming appropriation of the necessary amounts. Differences between the bills are reflected in the two cost estimates.

Estimate prepared by: Federal Costs: DHS—Mark Grabowicz; Coast Guard—Deborah Reis; Impact on State, local, and tribal governments: Sarah Puro; 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.

ADVISORY COMMITTEE STATEMENT

Section 2012 as created within Section 401 established the Advisory Council on Nuclear Detection as defined under section 5(b) of the Federal Advisory Committee Act. This section codifies the establishment of a new Advisory Council on Nuclear Detection.

The Advisory Council is to advise the Director of the Domestic Nuclear Detection Office on the global nuclear detection architecture. Members of the Advisory Council shall consist of individuals who possess expertise in nuclear and radiological detection, and are not employees of the Federal Government, other than employees of the National Laboratories. Members of the Advisory Council shall establish rules relating to conflict of interest within the Council.

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 Defence of the United States.

APPLICABILITY TO LEGISLATIVE BRANCH

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

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

TITLE I—SECURITY OF UNITED STATES SEAPORTS

SUBTITLE A—GENERAL PROVISIONS

Sec. 101. Definition of transportation security incident

This section clarifies the meaning of the term "transportation security incident" as defined by 46 U.S.C. §70101(6) to mean "a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area," by adding the text, "(other than economic disruption caused by acts that are unrelated to terrorism and are committed during a labor strike, demonstration, or other type of labor unrest)." The Committee seeks to ensure cargo and freight bound for the United States is not unduly delayed if no threat of terrorism or other unlawful activities are suspected during instances of labor unrest. Labor disputes, which have the potential to cause a transportation system or economic disruption, do not typically meet the definition of a "security incident."

Sec. 102. Protocols for resumption of trade

This section adds to the current requirements of the National Maritime Transportation Security Plan (NMTSP) under 46 U.S.C. §70103(a)(2)(J), which includes a plan to ensure "that the flow of cargo through United States ports is reestablished as efficiently and quickly as possible after a transportation security incident." The section requires that the NMTSP also provide guidance necessary to ensure plans for reestablishing the flow of cargo through United States ports are coordinated at the local, state, and regional level, and provide clear detail on government procedures in the event of a transportation security incident to minimize economic damage. A vague national plan will not provide adequate direction to allow the private sector to plan and respond. In New York Harbor, for example, the regional priority for the prioritization of the flow of goods in mid-January might be home heating oil products, whereas in the Port of Miami the priority may be containerized cargo with building materials.

The Committee recognizes the intermodal nature of ports, and intends that any resumption of trade program include an assessment of rail capabilities, rerouting, and other transshipment priorities. Setting these protocols will clearly involve Federal Government coordination, but also must include State and local priorities and integrate private sector capabilities.

It is imperative that port regions have realistic, workable resumption of trade plans and priorities established prior to an actual incident. Failure to have these plans in place will prove extremely costly in the event a transportation security incident occurs. Any lack of transparency and coordination will cause excessive delays in the resumption of commercial operations. The Congressional Budget Office estimates that (in 2004 dollars) a single day delay in imports at the Ports of Los Angeles and Long Beach could cost importers $4 million. If the disruption was such that all work stopped at the port, the resulting production loss would be between $65 and $150 million per day. The Committee believes it is critical that the Department of Homeland Security have plans in place to be able to quickly restore our ports to their maximum capacity in minimal time.

Sec. 103. Requirements relating to maritime facility plans

Subsection (a) requires that a security plan for a facility under 46 U.S.C. 70103(c) must be resubmitted for approval if the operation or ownership of the facility is transferred. Although the Maritime Transportation and Security Act of 2002 (MTSA), currently requires that facility and vessel security plans be updated every five years and resubmitted, "for approval of each change to the vessel or facility that may substantially affect the security of the vessel or facility," this section would mandate the resubmission of the security plan immediately upon the transfer of ownership or operation of any facility. The Committee finds that the security implications of a transfer of ownership or operation of a port facility constitutes sufficient cause for requiring the facility security plan to be resubmitted for review and approval.

Subsection (b) requires that the Facility Security Officer (FSO), as defined in 46 U.S.C. § 70103(c)(3)(B), be a citizen of the United States, unless the Secretary determines, after a complete back-

ground check of the individual and a check of the individual's name or alias against existing terrorist watchlists, that a waiver is appropriate. By virtue of the position, the FSO has special access to sensitive but unclassified information affecting port operations. The requirement that the FSO be a United States citizen provides some assurance that the person will not improperly divulge such information to a terrorist or other enemy of the United States. The Secretary is provided waiver authority under this provision to accommodate FSO applicants who are not United States citizens but may be especially well qualified for the position.

Subsection (c) requires the facility security plans under 46 U.S.C. § 70103(c)(3), incorporate provisions addressing access to secure areas of a vessel or facility for those engaged in surface transportation of containers, including truck drivers and those operating within rail facilities—provided those facilities fall within the boundaries outlined by the facility security plan.

Sec. 104. Unannounced inspections of maritime facilities

This section authorizes the Secretary of Homeland Security to conduct unannounced inspection of facilities at least once a year to verify the effectiveness of facility security plans. While the facility security plans outlined in 46 U.S.C. § 70103(c) are required to include a plan for "periodic unannounced drills," there is no similar requirement for unannounced inspections. Facilities are inspected annually, but the facility is usually given advance notice and the inspection is well-choreographed. While it is important to take into account the impact inspections have on industry, the Committee believes unannounced inspections are also required to ensure regular compliance. The unannounced inspections envisioned in this section are "spot checks" and should not be interpreted as full evaluations unless during the course of the spot check, the Coast Guard finds discrepancies in the execution of the facility security plan. If discrepancies arise, the Coast Guard should conduct a more thorough review of the facility security plan.

Nothing in this section is designed to preclude similar inspections for vessels and vessel security plans. While mandated under this section for facilities, the Committee recommends that similar actions be taken with vessels provided that due regard is given to the ship's schedule and the efficient flow of commerce.

Sec. 105. Verification of individuals with access to secure areas of seaports

This section closes a major gap in port security by requiring the Secretary of Homeland Security to implement the Transportation Worker Identification Credential (TWIC) as required by 45 U.S.C. § 70105. The Committee authorizes $20 million for Fiscal Year 2007 to begin implementation of the program. However, the Committee intends for this program to be supported through collected fees in future years.

This section requires that TWIC use Federally-issued access control cards to verify the identity of individuals with unescorted access to secure areas of U.S. seaports. The cards must be tamper-resistant, interoperable, and contain biometric information about the holder. Cardholders must successfully undergo a fingerprint-based background investigation. Each facility will determine which

workers are granted access to their secure areas and what level of access is permitted. The Committee supports the efforts of the Transportation Security Administration (TSA) and the U.S. Coast Guard to jointly implement this program and stresses that any further delays in implementation are unacceptable.

Subsection (a) requires the Secretary to issue a notice of proposed rulemaking (NPRM) for regulations to implement TWIC by July 15, 2006 and a final regulation by November 15, 2006. Under Subsection (b), the Secretary must begin issuing TWIC cards to individuals with unescorted access to secure areas of the 25 highest risk ports by May 15, 2007. The Secretary must begin issuing TWIC cards for the next 30 high-risk ports by November 15, 2007 and for all remaining seaport by November 15, 2008.

Subsection (c) requires the Secretary to complete named-based checks of all individuals with unescorted access to restricted areas of a seaport against the terrorist watchlists and relevant immigration databases no later than 90 days after the date of enactment. The Secretary shall issue an interim final rule to require appropriate entities to submit all necessary information for the Secretary to carryout the name-based checks. This subsection must be implemented in accordance with the Privacy Act in title 5 U.S.C. § 552(a). Any information obtained under this subsection shall remain confidential and may not be made available to the public, including the individual's employer. Given recent reports of individuals with fraudulent documents gaining access and employment at U.S. seaports, the Committee believes that an immediate check is essential while the TWIC program is implemented over the next several years.

Subsection (d) requires the Secretary to report to Congress within 120 days after enactment on the results of the interim check.

Subsection (e) requires the Secretary to reduce the fees associated with obtaining a TWIC card for those individuals who have successfully completed a background investigation for a Hazardous Material Endorsement (HME) under title 49 U.S.C. § 5103(a) and who hold a valid HME under 1572 of title 49 Code of Federal Regulations. The security threat requirements for the TWIC program and for the HME program are essentially the same. However, due to incompatible enrollment processes established by the Department, truck drivers who have already passed the HME background check will still be required to pay a large portion of the fees associate with obtaining a TWIC card. The Committee is concerned that this is a significant and unnecessary burden and directs the Secretary to take all necessary steps to consolidate these two programs and reduce the costs for drivers required to comply with both programs.

The Committee is concerned that Section 528 of the Department of Homeland Security Appropriations Bill (P.L. 109–90) requires the Secretary to utilize the Transportation Security Clearinghouse (TSC) as the central identity management system for deployment and operation of the registered traveler program and the TWIC program. Because the TSC is a private entity, the Committee is concerned about maintaining confidentiality of the personal information on TWIC applicants submitted to the TSC. The Committee expects that the TSC will not retain personal information on TWIC applicants for any period beyond that necessary for the processing

of applications. Additionally, the Secretary must ensure that the arrangement with the TSC complies with all privacy laws and regulations regularly. The Committee is aware of existing technology in use at the Department of Defense and the U.S. Coast Guard that is able to protect the privacy of sensitive data. The Secretary is directed to review and evaluate this technology for possible use in the TWIC program.

While the Committee applauds the Department for moving forward with the implementation of TWIC, the Committee is concerned about program delays. For this reason, the Committee encourages the Department to use, to the maximum extent possible, existing technologies and systems that have been employed in other venues to promote expeditious implementation of the program. Further, the Committee encourages the Department to maximize the use of small businesses as part of the final TWIC selection process. Small businesses often have the ingenuity, technology and flexibility to assist in the efficient implementation of a new and challenging program.

Sec. 106. Clarification on eligibility for transportation security cards

This section amends 46 U.S.C. §70105(c)(2) to clarify that the Secretary has no authority to grant a waiver for issuing a transportation security card to an illegal alien. The intent of this provision is to close a potential loophole in the framework for issuing transportation security cards, and eliminate any possible ambiguity over the Secretary's waiver authority.

Sec. 107. Long-range vessel tracking

This section amends title 46 U.S.C. §70115 to require the Secretary of Homeland Security to issue regulations that establish and implement a long-range vessel tracking system by not later than April 1, 2007. This system will have the capability to track vessels up to 2000 nautical miles from shore and will compliment the near-shore tracking capabilities provided by the Automatic Identification System (AIS). The U.S. Coast Guard is currently working through the International Maritime Organization (IMO) to develop the components of a global system rather than implementing a long-range vessel tracking system domestically. The Committee understands that the final system will have to be compatible with a system implemented by our international partners. However, the Committee remains concerned by the Administration's apparent decision to delay the development and implementation of this system in the United States. The Committee strongly recommends that the Coast Guard actively work through the IMO to develop standards and procedures. Failure to come to an agreement through the IMO should not deter the United States from implementing this critical maritime and port security measure domestically by the statutory deadline of April 1, 2007.

Subsection (b) authorizes the Secretary to establish a pilot program to track vessels who voluntarily agree to participate until such time as the program under this section becomes mandatory. The Committee strongly recommends the Secretary utilize the pilot program to test and evaluate technologies and procedures to fur-

ther the development of a mandatory, nationwide long-range vessel tracking system.

Sec. 108. Maritime Security Command Centers

This section amends title 46 U.S.C. to add a new Section 70118. This section requires the Secretary of Homeland Security to develop an integrated network of virtual and physical maritime security command centers at U.S. seaports and maritime regions for the purpose of enhancing information sharing, facilitating operational coordination, and facilitating incident management and response.

The U.S. Coast Guard has placed significant emphasis on upgrading their capabilities at the regional command centers around the country. The U.S. Coast Guard operates a National Command Center in Washington, DC, regional Area Command Centers on the east and west coasts, nine district command centers in regions such as Boston, Miami, Seattle, and Honolulu, and some thirty-six sector command centers, primarily focused in the port regions such as Baltimore, New York, Los Angeles/Long Beach, and Houston. Many of these command centers include video teleconferencing capabilities, access to classified intelligence community assessments, and extensive secure communications suites. Within these same regions, Customs and Border Protection, Immigration and Customs Enforcement, and their State and local counterparts often have only minimal resources in comparason. While this section does not mandate that the Coast Guard Sector Command Centers serve as the regional Maritime Security Command Center, the Committee has found these centers exceptionally capable and a logical starting point for this initiative.

Wherever possible, these integrated command centers should not involve building new facilities. It is the sense of the Committee that, where the co-location of personnel is necessary, the most capable sector, district, or area command center within a region utilize existing space to provide for the inclusion of appropriate federal agencies. If practicable, critical state and local agencies should also be included. It is the intent of the Committee that participation in these Command Centers will not require hiring of additional personnel, but shall focus on designating existing personnel to participate and utilize interoperable communications and the virtual network. Annual appropriations authorized for these facilities may be used to procure computer equipment, information technology, office furniture and supplies, and other necessary items to improve and expand the capabilities of existing centers.

When simple upgrades or modifications to existing facilities are not possible or sufficient office space is not available to provide for truly integrated operations, appropriations are authorized to develop a virtual, integrated communications system to ensure the maximum participation possible of other appropriate entities. These systems may include but are not limited to intranets, secure chat systems, and video teleconferencing capabilities.

This section also requires the Secretary to sponsor appropriate participants in the maritime command centers for security clearances. Should security clearances be required given the sensitive operations of these centers, those clearances will be sponsored by the Secretary of Homeland Security and shall include sufficiently

detailed background investigations to ensure their applicability with the Department of Defense requirements. While the Committee is aware that some State and local law enforcement officials will have already been vetted at the State or local level, the exceptionally sensitive nature of national security information is such that it requires an extensive, standardized, investigative process.

The section also provides that in the event of a transportation security incident involving a port, the Captain of the Port as designated by the U.S. Coast Guard, who is the head of the maritime security command center will act as the incident commander. The Captain of the Port will, therefore, direct response and mitigation efforts unless otherwise directed by the President in accordance with the National Response Plan, National Incident Management System, or the Maritime Operational Threat Response Plan applicable in the port region.

For each fiscal year from 2007–2012, $60 million is authorized to carry out this section. This section also requires the Secretary to submit a budget plan for implementing the maritime command centers, and outlining cost-share agreements with other Federal agencies.

SUBTITLE B—GRANT AND TRAINING PROGRAMS

Sec. 111. Port security grant program

This section establishes a new grant program under the Homeland Security Act (P.L. 107–296) specifically targeted to assist United States seaports in making necessary security enhancements to deter, prepare for, respond to, and recover from a terrorist attack. The total funding available for the grant program is $400 million per year over six years. Under the terms of this section, funding for this port security grant program will be derived from customs duties collected on incoming containers.

The grant program authorized under this section represents a substantial increase in the dedication of resources to port security. The Department of Homeland Security has awarded over $700 million in port security grant money to U.S. ports and an additional $168 million in grant awards will soon be announced, bringing total port security funding levels since September 11, 2001, to $870 million, since the September 11, 2001 terrorist attacks. This funding has provided significant support for needed port security enhancements. The port security grant program under this section more than doubles the amount of funding that has typically been available for grant awards in previous years. The additional support will allow for critical port security improvements at high risk and high priority ports within the United States to counter growing and immediate threats in the maritime sector.

The program requires the Secretary to allocate grant funds on the basis of risk and need, with special consideration given to ports with significant economic and defense importance. The new port security grant program under this section replaces the previous port security grant program established in Section 70105 of title 46 U.S.C., which required a fair and equitable allocation of grant funding.

While moving toward a risk-based approach, this section allows any entity subject to an Area Maritime Transportation Security

Plan to apply for grants and requires that each application meet minimum standards as required in the section. The last round of grants provided by the Secretary permitted funding for only the top 60 seaports based on a risk prioritization. While the Committee supports the risk-based allocation, it is important for each port to have the ability to apply and present its rationale for requesting grant funding.

This section permits grant money to be used to implement Area Maritime Transportation Security Plans, to remedy port security vulnerabilities, for salaries and operating expenses if the threat level or the Maritime Security (MARSEC) level is elevated, for acquisition and maintenance of security equipment, to conduct vulnerability assessments, to conduct counterterrorism training and exercise programs, to share threat information, to protect critical infrastructure, and for other security-related improvements. Grants may not be used for construction, land acquisition, or to make any State or local government cost-sharing contribution. The Secretary is authorized to award grants for multi-year projects. To ensure coordination within the ports and with the State, each grant award must be consistent with requirements of the Area Maritime Transportation Security Plan and any applicable State or Urban Area Homeland Security plan.

The Department of Homeland Security Inspector General has raised concerns in the past about lack of transparency in how grant money is utilized and on the types of projects being funded. This section responds to those concerns by requiring the Secretary to develop appropriate accounting and reporting procedures to track funding and ensure accountability. Additionally, all grant recipients are required to retain and make their records available to the Secretary for review and audit.

This section also requires the Secretary to limit the Federal contribution to port security grant projects to 75 percent of the total cost for all projects over $25,000, unless the Secretary determines it is appropriate to provide a higher level of Federal funding. Ports are also allowed to use expenses that are directly linked with the purpose for which the grant is awarded—including personnel overtime, contractor services, administrative costs, equipment fuel and maintenance, and rental space—to be counted towards the ports matching requirement.

Sec. 112. Port security training program

This section directs the Secretary to establish a Port Security Training Program for the purpose of ensuring that our Nation's emergency response providers, longshoremen, seaport management, the private sector, and others learn and master the skills necessary to prevent, prepare for, respond to, mitigate against, and recover from acts of terrorism, especially those involving weapons of mass destruction, natural disasters, and other emergencies.

The Port Security Training Program created by this section will use multiple mediums to provide validated training at the awareness, performance, and planning levels to emergency response providers and commercial seaport personnel and management. Specifically, the training program will address a variety of seaport security issues, including: (1) seaport security plans and procedures; (2) seaport security force operations and management; (3) physical se-

curity and access control at seaports; (4) methods of security for preventing and countering cargo theft; (5) container security; (6) recognition and detection of weapons, dangerous substances, and devices; (7) security threats and patterns; (8) procedures for communication with emergency response providers; and (9) evacuation procedures.

This section also amends the Maritime Transportation Security Act (P.L. 107–295) to require that all Vessel and Facility Security Plans include a strategy and timeline for conducting training and periodic unannounced exercises with respect to transportation security incidents. The Committee intends for each facility to fulfill the requirement under the Maritime Transportation Security Act, as amended by section 111(c) of this Act, to conduct training and periodic unannounced drills for persons on the vessel or at the facility through the use of, at a minimum, the courses, materials, and activities created or administered as part of the Port Security Training Program.

The Committee also intends that the level and type of training provided by the Department for government officials, commercial seaport personnel and management, and emergency response providers as part of the Port Security Training Program shall be in accordance with the duties and functions to be performed by each person in the event of an incident or emergency. The Secretary is expected to provide guidance to grant recipients and training partners under this program to ensure proper training levels. Training programs for emergency response providers should, at a minimum, include training at the performance and operations levels.

Sec. 113. Port security exercise program

This section requires the Secretary of Homeland Security to establish a Port Security Exercise Program for the purpose of testing and evaluating the emergency capabilities of Federal, State, local, and international governments, longshoremen, commercial seaport management, emergency response providers, and the private sector. Specifically, this section directs the Secretary to consolidate all of the Department of Homeland Security's existing port security exercise programs. It also requires the Department to conduct, on a periodic basis, port security exercises that are: (1) tailored to the needs of each port; (2) as realistic as possible; (3) evaluated against clear and consistent performance measures; (4) assessed to learn best practices; and (5) followed by remedial action.

This section directs the Secretary to ensure that all port security exercises are consistent with the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Infrastructure Protection Plan, and other such national initiatives. Moreover, such exercises must be consistent with any applicable Area Maritime Security Transportation Plans and State or urban area homeland security strategy or plan.

Finally, this section directs the Secretary to establish a Remedial Action Management System to: (1) identify and analyze each port security exercise for lessons learned and best practices; (2) disseminate lessons learned and best practices to participants in the exercise program; (3) monitor the implementation of lessons learned

and best practices by program participants; and (4) conduct remedial action tracking and long-term trend analysis.

The Committee has repeatedly heard from emergency response providers across our Nation about the importance of conducting table-top and full-scale exercises to test and evaluate our preparedness and response capabilities. The value of exercises cannot be understated. The success or failure of our response to acts of terrorism, natural disasters, or other emergencies depends on effective coordination and cooperation. It is simply too late for emergency response providers to develop working relationships during an actual event.

Sec. 114. Reserve officers and junior reserve officers training pilot project

This section permits the Secretary to initiate a pilot project and establish and maintain reserve officer and a junior reserve officers training program at nine locations (Coast Guard Districts) around the country. The provision requires at least one location be at a historically black college or university, and a second at a high-school with a large minority population.

SUBTITLE C—MISCELLANEOUS PROVISIONS

Sec. 121. Increase in port of entry inspection officers

This section authorizes 1,200 additional U.S. Customs and Border Protection (CBP) Officers at U.S. ports of entry over six years. There are currently 19,000 inspectors responsible for 317 ports of entry, 14 pre-clearance stations, and assignments to the 44 foreign ports under the Container Security Initiative. While other border security positions in the Department of Homeland Security were enhanced in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108–458), the number of CBP Officers was not increased. The Committee supports additional staffing at ports of entry to ensure that thorough security screenings for individuals and cargo are maintained without disrupting the legitimate flow of goods. Additionally, more personnel will be necessary to carry out new requirements established under this measure, including enhancing targeting capabilities, collection of additional advanced data, and expansion of the Container Security Initiative (CSI).

This section mirrors a provision included by the Committee in Section 107 of H.R. 4437, the Border Protection, Antiterrorism and Illegal Immigration Control Act of 2005, which passed the House of Representatives on December 16, 2005. This provision was also included in H.R. 4312, the Border Security and Terrorism Prevention Act of 2005, which was reported by the Committee on Homeland Security on December 6, 2005.

This section authorizes $20 million for Fiscal Year 2007, and increases that authorization by $20 million each subsequent fiscal year through 2012 for a total funding amount of $420 million over six years.

Sec. 122. Acceleration of Integrated Deepwater System.

This section increases the authorized funding for the Coast Guard's Deepwater System by $1.892 billion. The Integrated Deepwater System is the Coast Guard's largest capital acquisition pro-

gram, touted as a "system of systems" approach to rebuilding and replacing its aging fleet of ships and aircraft. The President's budget request for the Deepwater System is $934 million in 2007, and increase in $11 million from 2006 funding levels. This funding level supports the 25-year recapitalization timeline.

The Committee supports the acceleration of the Deepwater System in concept and recognizes the important multi-mission role which requires the service to use the same aircraft and vessels for port and waterways security as it uses for search and rescue, drug interdiction, and general law enforcement activities.

Sec. 123. Border Patrol unit for United States Virgin Islands

This section establishes a Border Patrol unit for the United States Virgin Islands as a means to enhance security and awareness. No Border Patrol station currently exists within the territory of U.S. Virgin Islands and the station responsible for covering this area is located in Puerto Rico. The United States Virgin Islands has 175 miles of coastal borders and is a gateway to the continental U.S. This region has been increasingly exploited by human and drug smugglers to move people and narcotics, undetected, into the U.S. mainland. A dedicated Border Patrol unit will assist the Department of Homeland Security in gaining operational control over the border.

Sec. 124. Report on ownership and operation of United States seaports

This section requires the Secretary of Homeland Security to submit a report to Congress within 180 days with the name of each individual or entity that leases, operates, manages or owns property or facilities at seaports. During a recent review of the Committee on Financial Investment in the United States' (CFIUS) approval of Dubai Ports World acquisition of several terminal operations in the United Sates, the Committee became concerned about the inability of the Department of Homeland Security or any other entity to provide data on the number of foreign operated terminals in the United States. The purpose of this section is to ensure that Congress and the Department have the all necessary information to evaluate security at United States seaports.

Sec. 125. Report on security operations at certain United States seaports

This section requires the Secretary of Homeland Security to conduct a study and provide a report to Congress within 270 days on the adequacy of security operations at the ten largest container ports in the United States as a means of reviewing current vulnerability assessments completed by the Coast Guard to ensure they are sufficient in scope and accurately assess the security of our ports with the largest volumes of container traffic.

Sec. 126. Report on arrival and departure manifests for certain commercial vessels in the United States Virgin Islands

This section requires the Secretary of Homeland Security to provide a report to Congress on how the requirements under section 231 of the Immigration and Nationality Act (8 U.S.C. 1221) relating to filing of arrival and departure manifests, impacts small com-

mercial vessels operating between the U.S. and British Virgin Islands. The Committee is concerned that the Department does not fully consider the impact of small businesses when implementing nationwide security requirements and directs the Secretary to fully consider the impact on charter boats and small yachts of requirements to file manifest data one hour prior to arrival and departure.

TITLE II—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN

Sec. 201. Security of the international supply chain

This section amends the Homeland Security Act of 2002 (P.L. 107–296) to establish Title XVIII, designated as "Security of the International Supply Chain." The provisions in this section reinforce the importance of improving security and providing the Secretary with clear direction and enhanced authorities to prevent, detect, respond to and recover from a terrorist threat to the international supply chain and the maritime transportation system.

SUBTITLE A—GENERAL PROVISIONS

Sec. 1801. Strategic plan to enhance the security of the international supply chain

This section requires the Secretary of Homeland Security to establish a strategic plan for enhancing the security of the international supply chain. Over 11 million containers are expected to enter the United States this year through U.S. seaports. The importance of maintaining the flow of commerce and the consequences of a weapon of mass destruction being smuggled into the U.S. in one of those containers requires focused attention on container and supply chain security.

The strategic plan required under this section is required to address the roles and responsibilities for each public and private stakeholder responsible for the security of the movement of containers, identify and address security gaps, provide legislative recommendations, provide goals for improving security from the point of origin to the point of destinations, recommend incentives for additional voluntary measures, consider the impact on small businesses of security requirements, include a process for sharing security information with the private sector, identify a response plan, and consider possible linkages between supply chain security and travel and financial security. Recognizing the strategic planning already underway in the National Strategy for Maritime Security (NSMS), this section requires that the International Supply Chain Strategy expand upon and relate to the goals and priorities established in the NSMS. Section 201(c)(1) requires that the Strategy be complete and provided to the Committee within 180 days of enactment.

Sec. 1802. Transmission of additional data elements for improved high risk targeting

This section requires the Secretary to issue regulations within one year to require additional data elements, including entry data to be provided electronically to the Department prior to loading cargo on vessels bound for the United States. This regulatory au-

thority includes determining the appropriate security elements of entry data. The intent of this provision is to improve the capability of Secretary to identify high risk cargo, an essential element of the U.S. maritime security strategy. This provision provides the Secretary with clear authority and direction to collect additional data and sufficient flexibility to determine what data should be required to enhance capabilities to detect high risk cargo.

The Committee has conducted extensive oversight of Automated Targeted System and the data elements utilized by U.S. Customs and Border Protection (CBP) to identify high risk containers, and determined that the existing reliance on carrier manifest data is insufficient to ensure robust targeting capabilities. This section takes steps to resolve this issue by empowering the Secretary to improve the risk-based targeting system through the collection of additional data.

Currently, no data is required to be filed prior to loading by a U.S. importer or foreign exporter that can be used in the security screening process. However, these parties possess shipment data that security experts testified would add significant targeting capabilities. Today, cargo entry data is required to be filed with CBP by the importer, but is not required to be filed until after the cargo shipment is in the United States, which is too late to be used for security screening purposes. However, the Department has not acted to require this information be submitted.

Sec. 1803. Plan to improve the Automated Targeting System

This section requires the Secretary, within 180 days to develop a plan to improve the Automated Targeting System (ATS) to enhance capabilities to detect high-risk containers. The plan may include requiring additional non-manifest documentation and reducing reporting timelines for each container. Additionally, the Secretary shall require an outside peer review of the system. This section is intended to ensure that additional consideration is provided to improving ATS in addition to the additional data required in Section 1802 of this subtitle. To provide for necessary improvements to ATS, the Committee authorizes $5 million to be dedicated to the system for each fiscal year from 2007–2012.

The Government Accountability Office (GAO) issued a report titled, "Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection" (GAO–04–557T), and noted that U.S. Customs and Border Protection (CBP) "has not performed a comprehensive set of threat, criticality, vulnerability, and risk assessment," nor has CBP "subjected the targeting system to external peer review or testing." In the context of implementing a plan to improve ATS, the Secretary is directed to address the recommendations made in the GAO report to and evaluate the need for other changes to ATS including requiring additional data and adjusting the timing for submitting the additional data.

The Committee also supports the recommendations made by the Commercial Operations Advisory Council (COAC) Maritime Transportation Security Act Advisory Subcommittee in September 2004. The Committee directs the Secretary to evaluate these recommendations, which specify that importers should provide CBP additional data elements before vessel loading, including (1) a bet-

ter cargo description; (2) the identity of the party that is selling the goods to the importer; (3) the identity of the party that is purchasing the goods; (4) point of origin of the goods; (5) country from which the goods are exported; (6) identity of the ultimate consignee; (7) identity of the exporter representative; (8) identity of the broker; and (9) the origin of the container shipment.

The Secretary shall continually review ATS and upgrade the system as more complex targeting capabilities become available and seek to incorporate real-time intelligence into the system. The Committee specifically directs the Secretary to review whether ATS can, and should, be linked with existing terrorist travel and finance programs to allow for patterns and connections that may otherwise be missed.

Finally, the Committee directs the Secretary to consult with appropriate stakeholders, including the Homeland Security Advisory Committee, the National Maritime Security Advisory Committee, and the Commercial Operations Advisory Committee, when considering what additional information may be required and to ensure that all information submitted be transmitted and stored in a secure fashion.

Sec. 1804. Container standards and verification procedures

This section requires the Secretary of Homeland Security to establish minimum standards and verification procedures for sealing containers imported into the United States within 180 days of enactment. Two years from enactment, the Secretary must require the enforcement of those standards on all containers entering the United States. Currently the U.S. imports over 11 million containers annually. The current internationally approved method for sealing those containers is a small, serialized bolt seal. Relatively easy to circumvent, these seals do not provide adequate security. As regional instability continues in Eastern Europe, portions of Asia, Africa, and the Middle East, the threat of independent terrorist activities by non-state actors grows. Many security experts believe that the container supply chain is vulnerable to being exploited by terrorists.

The Committee is concerned that the state of current technology in this realm is currently insufficient. Technologies that can detect the unauthorized opening or exploitation of a container are still evolving. Ideally, container security devices could provide advanced warning of evidence of tampering and be tracked real time. Current container security devices show significant improvements over the serialized bolts but still only protect the container door. Advanced devices and electronic seals being tested are currently too expensive to be widely used in the supply chain. The Secretary is directed to continue to test commercially available technology and develop the best available standards for sealing and protecting containers that can be implemented in the supply chain. The Committee understands that these capabilities may not be available immediately, but directs industry to lead the way, as these systems will also prevent theft of increasingly high-cost items shipped in these containers. It is critical that new technologies for securing containers minimize false positive readings, and ideally incorporate a false-positive of less than one percent. It is equally critical that the Secretary incorporate procedures for reconciling alarm data

which would not unduly disrupt commerce. In developing standards under this section, the Secretary shall consult with private sector stakeholders, including the Homeland Security Advisory Committee, the National Maritime Security Advisory Committee, and the Commercial Operations Advisory Committee.

Given that the container supply chain is global in scope, the Committee encourages the Secretary to work with international organizations and foreign governments to ensure that the standards established by the Department are consistent with those being developed internationally. However, the Secretary shall not delay action if international consensus cannot be reached. While the Committee requires that the Secretary not violate international trade obligations, the United States must lead the effort to improve global supply chain security.

Sec. 1805. Container Security Initiative

This section authorizes the establishment and implementation of the Container Security Initiative (CSI) to identify and examine maritime containers at foreign ports that may pose a risk for terrorism before the containers are shipped to the United States. This program has been operational since 2002 and has processed nearly 20 million containers through 44 foreign ports. By the end of 2006, approximately 82 percent of all imported containerized cargo will pass through a CSI-designated port. The CSI program effectively pushes our security effort out beyond the geographic borders of the United States to increase opportunities to detect high risk containers before they are loaded overseas and arrive at our ports. The Committee commends the Department of Homeland Security for establishing this outreach program and supports its continuation and expansion by authorizing $196 million each year for fiscal year 2007–2012.

This section provides that, as a prerequisite for designating a CSI port, the Secretary of Homeland Security must ensure an appropriate port assessment is completed and that CSI assessments are coordinated with the U.S. Coast Guard's regular foreign port assessments to ensure that all available information is utilized in determining the location of CSI ports and to minimize disruptions with the host nation. The Committee directs the Secretary to notify Congress of the designation of any CSI port prior to the public announcement.

This section also allows the Secretary to provide foreign assistance and equipment loans to host nations that are unable to purchase inspection equipment that meet the standards established by the Department. Non-intrusive imagery and radiation detection equipment can prove cost prohibitive for some nations. The systems currently cost between $1.5 million and $3.0 million. The Secretary may loan, purchase, or otherwise offset the costs of these technologies and provide necessary training and refresher training to foreign personnel involved in the CSI program.

With the continuously improving technology in the fields of non-intrusive imagery and radiation and nuclear detection, the Committee directs the Secretary to periodically reassess available technology and utilize the enhanced systems as old systems become obsolete. At a minimum, the Secretary is directed to ensure that each

CSI port have capabilities for non-intrusive imaging (i.e. x-ray or gamma ray) and nuclear and radiological detection.

The Committee is concerned that several CSI host nations are not compliant with requests to scan containers that the U.S. deems to be high risk. For example, at the Port of Shanghai, China, U.S. Customs and Border Protection (CBP) selected 2,103 containers for scanning, but the host government refused to scan 586 of the requests. To address this issue, the Committee requires the Secretary to issue a "do not load" order for any container targeted as high risk if the host government refuses to inspect.

The Committee requires the Secretary of Homeland Security to submit an annual report on the progress of the CSI program. The report must include a description of security improvements to the program, the rationale for continuation at each CSI port, and an assessment of personnel needs. The Committee is concerned that the program may expand beyond the need and directs the Secretary to evaluate options for utilizing CBP targeters in the United States when possible rather than assigning large CSI teams overseas, which nearly triples personnel costs. Additionally, the Committee directs the Secretary to assess opportunities to enhance CSI through exploring capabilities to electronically send images and data between the U.S. and CSI ports for use in the Automated Targeting System.

Sec. 1806. Information sharing relating to supply chain security cooperation

This section requires the Secretary to establish a secure system to share and receive supply chain security information from the private sector. The Committee is concerned that the Department provides little or no risk information to the private sector to assist them in hardening and adjusting their supply routes. This section will enhance cooperation between the Department and the private sector in a secure, web-based system that will protect data and the identity of the private sector entities providing information. The Secretary shall consult with the private sector in developing the system.

The Secretary is directed to review the web system established by the Department of State's Overseas Security Advisory Council. The Committee directs the Secretary to build on this model to establish a continuing liaison with the private sector and to provide regular interchange of information.

Information shared through this system may be sensitive and proprietary. The Secretary shall exempt information received through the system from public disclosure. Any warnings that the Secretary may issue through the system based upon information received, shall not include identifiable information related to the submitting entity.

SUBTITLE B—CUSTOMS—TRADE PARTNERSHIP AGAINST TERRORISM (C–TPAT)

Sec. 1811. Establishment

This section authorizes the Customs-Trade Partnership Against Terrorism (C–TPAT) program. C–TPAT was initiated in November 2001, and involves voluntary agreements with major importers,

shippers and other entities whereby they agree to establish certain protocols and processes for improving international supply chain security at their facilities and the federal government provides benefits in the form of decreased cargo inspection rates and other commercial benefits. Today, the program has over 10,000 applicants and more than 5,600 certified participants.

The Committee, while supportive of the program, has identified several problems with the C–TPAT program, and requires the Secretary to evaluate and, where appropriate, implement the recommendations of the Government Accountability Office (GAO) report entitled "Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security" (GAO–05–404). The Secretary is also required to develop minimum security requirements for C–TPAT participation and review the requirements at least once a year and update as necessary.

Sec. 1812. Eligible entities

This section includes a list of private sector entities that are eligible to participate in the Customs-Trade Partnership Against Terrorism (C–TPAT). Participants include importers, brokers, freight forwarders, air, sea, land carriers, and any other entity in the international supply chain or intermodal transportation system can apply to enter the C–TPAT program.

Sec. 1813. Minimum requirements

This section identifies specific criteria for applicants to participate in the Customs-Trade Partnership Against Terrorism (C–TPAT). In addition to other requirements identified and established by the Secretary of Homeland Security, the criteria include a demonstrated history of international commerce. The Committee intends that C–TPAT participants have a two-year history at a minimum, which would provide adequate historical data for the Department to determine whether the applicant has a good track record and if any derogatory intelligence has been found regarding the entity. The applicant must also complete an assessment of supply chains under the C–TPAT program which must consider, at a minimum, business partner requirements, container security, physical security and access controls, personnel security, procedural security, security training and threat awareness, and information technology security. The Committee intends for the Secretary to use the minimum requirements as a baseline and establish additional criteria as appropriate. It is through the minimum requirements of site access, training, and other security measures that the supply chain back to the point of origin is strengthened and transparency is attained.

Sec. 1814. Tier One Participants

This section establishes an initial level, or "Tier One" of the Customs-Trade Partnership Against Terrorism (C–TPAT) program. A C–TPAT member is eligible to receive Tier One status after applying for the program and being certified by the Secretary of Homeland Security. The Secretary is required to establish criteria and guidelines for the certification process. The Committee intends the certification process to consist of more than a paperwork review. It is essential that the certification include a thorough review of the

all available information on the entity and its primary managers, owners, and decision makers.

Since Tier One members have not received a validation as required under Section 1815 of this subtitle, any program benefits should be limited in nature and should be commensurate with the level of scrutiny received in the certification process. The Committee intends that Tier One participants receive significantly few benefits than for Tier Two (established in Section 1815) or Tier Three (established in Section 1816). The Tier One benefit is to provide an incentive for eligible entities to sign up and should not greatly impact a Tier One participant's number of inspections.

Sec. 1815. Tier Two Participants

This section establishes a second level or "Tier Two" of the Customs-Trade Partnership Against Terrorism (C–TPAT) program. Within one year of becoming a Tier One member (established in Section 1814), the Secretary of Homeland Security must conduct a validation of the security measures of the participant. The validation must include on-site checks at various points along the participants supply chain, including foreign locations. The Committee is concerned that some foreign countries are refusing to provide access to U.S. Customs and Border Protection (CBP) personnel conducting the validations. The Committee directs the Secretary of Homeland Security, in consultation with the Secretary of State, to work with those nations to open up access to ensure security to the point of origin to the extent feasible.

If a C–TPAT participant fails the validation, the CBP Commissioner may expel the participant or deny benefits under the program, which may include reduced examinations and priority for searches. The Secretary of Homeland Security shall establish a mechanism for a C–TPAT participant to appeal a denial of benefits or expulsion.

Sec. 1816 Tier Three Participants

This section establishes a third level or "Tier Three" of the Customs-Trade Partnership Against Terrorism (C–TPAT) program. The Committee realizes that some C–TPAT members establish procedures above and beyond the minimum requirements and may demonstrate a sustained, superior effort through investing independently in advanced technologies or instituting process which further improve supply chain security. Those participants exceeding the minimum criteria established by the Secretary should receive greater benefits. The Secretary shall consult with the Commercial Operations Advisory Committee and the National Maritime Security Advisory Committee to determine appropriate benefits and within two years of enactment, the Secretary shall determine which additional benefits to provide.

Among the benefit options, the Secretary shall consider providing the participant expedited release of their goods provided such actions are consistent with the Protocols for the Resumption of Trade outlined in 46 U.S.C. §70103(a)(2)(J), reduced or streamlined bonding requirements if consistent with obligations under other applicable provisions of law, a higher level of reduced examinations, priority over Tier One and Tier Two participants if selected for additional scanning or inspection, further reduced scores in the Auto-

mated Targeting Systems, and streamlined billing of customs duties or fees.

Sec. 1817. Consequences for lack of compliance

This section establishes consequences if a Customs-Trade Partnership Against Terrorism (C–TPAT) member is not in compliance with the guidelines of the program. Subsection (a) allows the Secretary to deny benefits to the C–TPAT participants if their security measures fail to meet the program requirements. Subsection (b) provides penalties for participants who intentionally provide false or misleading information. If the Secretary determines that a C–TPAT member intentionally provided false information, that member shall be removed from the program for not less than five years. Subsection (c) provides an opportunity for appeal for a C–TPAT member who has been found to be in violation of the rules of the program and denied benefits or removed from the program.

Sec. 1818. Validations by third party entities

This section authorizes the Secretary of Homeland Security to C–TPAT members to contract with certified third parties to conduct validations of Customs-Trade Partnership Against Terrorism (C–TPAT) members. The requirements of this section apply to both the pilot program authorized under this subtitle as well as the expanded general use of third parties to conduct validations upon the successful completion of the pilot program.

The Committee believes that the authorizing of third parties to conduct C–TPAT validations will harness the potential efficiencies and cost savings of involving responsible non-federal organizations in the validation process. Currently, U.S. Customs and Border Protection (CBP) has a limited number of inspectors and contract employees available to perform validations, and a significant backlog of participants awaiting validation. Expanding the validation effort through the use of third parties should accelerate the timetable for validation and hasten the availability of Tier Two benefits available to validated C–TPAT participants.

Prior to initiating the pilot program under this section, the Secretary is required to develop and update minimum standard operating procedures for third party validations. These procedures should replicate and where possible improve upon the processes and procedures currently utilized by CBP in carrying out the C–TPAT validations. The Secretary must submit the standard operating procedures (along with necessary supporting information) for a technical review by the Office of SAFETY Act Implementation (or other appropriate components of the Department), and ensure that all necessary steps are taken to secure the designation of the standard operating procedures as a qualified anti-terrorism technology under the SAFETY Act [Subtitle G of title VIII of the Homeland Security Act of 2002 (P.L. 107–296).

Once the standard operating procedures have been developed and designated, the Secretary shall make them available to third parties who seek to perform validations as part of the C–TPAT program. The Secretary shall then issue certificates of conformance to third parties who demonstrate the ability to perform and agree to perform validations in accordance with those standard operating procedures, maintain liability insurance in the amount established

by the Secretary as part of a request for certification; and agree to protect all proprietary information of C–TPAT participants from disclosure.

The issuance of the certificate of conformance entitles the third party validator to all of the litigation and risk management protections of the SAFETY Act. The Secretary is required to monitor and inspect the operations of third party entities conducting validations to ensure they continue to meet minimum standard operating procedures. If the Secretary finds a third party validator is not meeting the minimum requirements, the Secretary shall revoke the certificate of conformance and review any validation conducted by the entity.

This section further clarifies that parties to the third party validation contracts are to involve the third party validator and the C–TPAT participant. The Department is not to be a party to the validation contract, nor responsible for the cost of the validations. The participant will pay all costs associated with the validation. In order to eliminate conflicts of interest and possible collusion, this section also requires that third party validators be independent of the C–TPAT participants they are validating.

Sec. 1819. Revalidation

This section requires the Secretary of Homeland Security to establish a process for revalidation of participants in the Customs-Trade Partnership Against Terrorism (C–TPAT) program not less than once every three years following the initial validation as required in Section 1818 of this subtitle.

Sec. 1820. Non-containerized cargo

This section authorizes the Secretary of Homeland Security to consider expanding the Customs-Trade Partnership Against Terrorism (C–TPAT) to allow participation from importers of non-containerized cargoes that meet the requirements in this subtitle. The Committee directs the Secretary to specifically review if the C–TPAT program would provide significant improvements for liquid cargo, such as oil and gas, as well as roll-on/roll-off cargo.

Sec. 1821. Authorization of appropriations

This section authorizes $75,000,000 to be provided for each of the fiscal years 2007 through 2012 to carry out this subtitle on the Customs-Trade Partnership Against Terrorism.

SUBTITLE C—MISCELLANEOUS PROVISIONS

Sec. 1831. Research, Development, Testing & Evaluation efforts in furtherance of maritime and cargo security

This section requires the Secretary of Homeland Security to direct research and development efforts to improve maritime and cargo security, encourage ingenuity and participation of the private sector, and evaluate technologies. The Committee is concerned about the lack of progress in developing and utilizing new container security technologies and the lack of transparency in the Department's current efforts. This section is intended to ensure that the Science and Technology Directorate, working with the Director of the Domestic Nuclear Detection Office of the Department (estab-

lished in Section 301) and other appropriate Department components coordinate these research and development efforts, and that results are shared across the Department, as well as with other appropriate Federal, State and local agencies.

Recognizing that we must be aggressive in protecting United States seaports, the Committee recommends that the Secretary conduct research and development on technology to automatically scan identification devices on containers entering and exit U.S. ports and to cross reference the appropriate identification device to the proper commercial data filed with U.S. Customs and Border Protection. Additionally, the Committee recommends that the Secretary establish a pilot program to evaluate the security benefit of such technology with appropriate port security and law enforcement agencies with responsibilities for the tracking, monitoring and security of cargo containers and securing port perimeters.

Sec. 1832. Operation Safe Commerce

This section requires the Secretary of Homeland Security to provide grants to the private sector under Operation Safe Commerce. The goal of this program is to encourage the integration of technologies, test access controls and create data sharing capabilities. The Secretary should utilize this program to promote public-private partnerships between ports, federal, state and local governments, and the private sector to identify, test and implement next-generation technologies related to supply chain security in the operational environment. As part of Operation Safe Commerce, the Secretary shall establish demonstration projects to enhance security and shall include projects on securing refrigerated containers, non-containerized cargo, roll-on/roll-off, and liquid cargo.

The Secretary shall award grants under this section on a competitive process based on criteria set forth in the legislation. Additionally, the Secretary shall ensure that grants are coordinated with other federally funded research projects in this area to avoid duplication and wasteful spending. Grant recipients must maintain records of expenditures and the Secretary shall annually review projects carried out under the program and report to Congress detailing the results of Operation Safe Commerce.

This section authorizes $25,000,000 for Operation Safe Commerce for each of fiscal years 2007 through 2012. However, this section requires that before new grants may be awarded under Operation Safe Commerce, the Secretary must report to Congress on the implementation and results of grants previously awarded under the program prior to the enactment of this Act. The Committee has been frustrated with the lack of information available on the status and lessons learned from Operation Safe Commerce grant projects funded in fiscal year 2002 and 2003, and this reporting requirement is intended to bring accountability to the program.

Sec. 1833. Definitions

This section defines key terms used in this title, including "Automated Targeting System," "examination," "inspection," "international supply chain," "nuclear and radiological detection system," "screening," and "search."

Sec. 202. Next generation supply chain security technologies

This section requires the Secretary of Homeland Security to continue risk-based screening, scanning, and inspecting of cargo while simultaneously evaluating nuclear and radiological detection, imagery, density, and other appropriate technologies for their commercial viability and use at foreign ports. Not later than one year after enactment of this provision, the Secretary is required to determine if technology is available that has a sufficiently low false alarm rate for use in the supply chain; is capable of being deployed and operated at ports overseas; is capable of integrating, where necessary, with existing systems; does not significantly impact trade capacity and flow of cargo at foreign or United States ports; and provides an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel. If such technology is available, this section requires that the Secretary, in cooperation with the Secretary of State, seek international cooperation to implement the use of the technology at foreign ports. In order to secure international cooperation, the Secretary is empowered to refuse containerized cargo from ports that refuse to cooperate. This section also requires the Secretary to submit a report to appropriate congressional committees on the evaluation and implementation of suitable technology, and an assessment of the level of cooperation of foreign governments.

The intent of these provisions is to provide a realistic framework for moving forward with technology capable of inspecting higher volumes of cargo at foreign ports than is currently available. Some members of the Committee have suggested that Congress should require 100 percent inspection and scanning of cargo bound for the United States within a fixed time frame. The Committee opposes such a requirement. While such a goal is admirable, it is simply unrealistic in the current environment, given the need for international cooperation, shortcomings in existing technology, and the need to avoid disrupting the flow of commerce and damaging the global economy. The framework established under this section provides a more realistic way forward on this important issue.

Sec. 203. Uniform data system for import and export information

This section requires the President to establish a single, uniform data sharing system for collection, dissemination, and sharing of import and export information. Since 1995, the federal government has been in the process of developing the International Trade Data System (ITDS) to be a government-wide system for the electronic collection and dissemination of international trade and transportation data for use by appropriate Federal agencies. The idea behind ITDS is to be a clearinghouse of information and facilitate private sector reporting mandates by providing a single interface and common data requirements. Currently, trade entities are required to submit data to multiple federal agencies in different formats, with different data requirements, and on different timelines. The United Nations Conference on Trade Development has estimated that the submission of redundant information and preparation of documentation is equal to 4–6 percent of the cost of the merchandise.

The Committee has been frustrated by the lack of progress in establishing ITDS. The Committee directs the President to push

other federal agencies to participate in the system and to consult with private sector stakeholders, including the National Maritime Security Advisory Committee and the Commercial Operations Advisory Committee, to develop uniform data requirements and procedures for ITDS. The President shall report to Congress on the status and implementation of ITDS within 120 days of enactment.

Sec. 204. Foreign Port Assessments

The Secretary of Homeland Security is required to conduct foreign port assessments to determine the effectiveness of antiterrorism measures under title 46 U.S.C. §70108. The current statute does not require a reassessment, though the U.S. Coast Guard had planned on conducting reassessments every five years. The Coast Guard has approximately 20 inspectors who complete these assessments. This section requires the Coast Guard to conduct reassessments every three years. It is this Committee's intent the Coast Guard reallocate the required resources to meet this mandate, anticipating a need to double the number of inspectors to meet the new three-year mandate.

Sec. 205. Pilot program to improve the security of empty containers

This section requires the Secretary of Homeland Security to conduct a one-year pilot program to evaluate the need to provide additional security of empty containers using visual inspections. Under current regulations, containers declared as empty are not generally inspected by Customs and Border Protection officials to ensure that they are actually empty. Within 90 days of the completion of the pilot program, the Secretary shall provide a report to Congress which must include recommendations on what actions are necessary to close this gap in our maritime border security.

Sec. 206. Study and report on advanced imagery pilot programs

This section requires the Secretary of Homeland Security to conduct a study on current container inspections pilot programs. The study should evaluate the cost, personnel and other resources that would be required to implement such programs to screen all cargo imported from foreign ports and to validate the data by U.S. Customs and Border Protection (CBP) personnel. The Secretary shall summarize best practices found in the pilots that could be integrated into the Container Security Initiative and other U.S. security programs. The Committee is interested in how existing security programs could be improved through refined targeting capabilities and increased container inspection rates. The Committee is concerned that insufficient information and modeling exists to fully understand the impact of such programs on the supply chain and the actual security value that would be provided. The Committee was encouraged to receive testimony before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity on March 16, 2006, from Mr. Jayson Ahern regarding CBP's plans to evaluate existing programs. The Committee intends for the study and report, which shall be submitted to Congress not later than 60 days after enactment, to include the results of that evaluation.

TITLE III—DIRECTORATE FOR POLICY, PLANNING, AND INTERNATIONAL AFFAIRS

Sec. 301. Establishment of Directorate for Policy, Planning, and International Affairs

This section authorizes the establishment of a Directorate for Policy, Planning, and International Affairs within the Department of Homeland Security. In March 2005, the Secretary of Homeland Security initiated a comprehensive review of the Department's structure, operations, and activities. Pursuant to this review—referred to as the Second Stage Review or 2SR—the Secretary recommended the establishment of a Department-wide policy office headed by an Under Secretary for Policy who would report directly to the Secretary.

This provision establishes the recommended policy office as the Directorate for Policy, Planning, and International Affairs, to be administered by an Under Secretary for Policy. The individual appointed as Under Secretary shall have, by education and experience, demonstrated knowledge, ability and skill in the fields of policy and strategic planning.

Among other things, the Under Secretary for Policy shall be responsible for: policy development and coordination, including providing overall direction and supervision of policy development, establishing and implementing a formal policymaking process, and ensuring that the Department's budget is aligned with its statutory and regulatory responsibilities and the Secretary's priorities; strategic planning, including conducting long-range planning, preparing national and Departmental strategies, and conducting net assessments of issues facing the Department; international activities of the Department, including promoting information exchange, planning and participating in international conferences and exchange programs, and overseeing the activities of Department personnel operating overseas; and communication with the private sector, including fostering strategic communications to enhance the Department's primary protective mission, advising the Secretary on the impact on the private sector of Departmental policies and regulations, and creating and managing private sector advisory councils.

This section transfers the Office of International Affairs, established in Section 879 of the Homeland Security Act of 2002 (P.L. 107–296), and elevates the office's director to the rank of Assistant Secretary. This section also establishes the following offices and positions within the Directorate: an Office of Policy, to be administered by an Assistant Secretary for Policy; an Office of Strategic Plans, to be administered by an Assistant Secretary for Strategic Plans, and which will include a Secure Border Initiative Program Office and a Screening Coordination and Operations Office; an Office of the Private Sector; a Victim Assistance Officer; a Tribal Security Officer; and a Director of Cargo Security Policy.

The Victim Assistance Officer will coordinate and serve as the point of contact for individuals affected by a terrorist attack or natural disaster and their families. The Victim Assistance Officer will coordinate with relevant officials throughout the Department to facilitate the dissemination of information regarding assistance programs and other forms of aid that may be available in the wake

of a disaster, as well as to coordinate other concerns raised by affected individuals. The Victim Assistance Officer also will coordinate Departmental responses to victims with similarly situated officials at the Federal Bureau of Investigation, the National Transportation Safety Board, and other Federal agencies which respond to an act of terrorism or natural disaster.

The Tribal Security Officer will serve as the single point of contact for tribal governments across the United States and its territories. Currently, Indian tribes, as defined by section 4(e) of the Indian Self-Determination and Education Assistance Act, 25 U.S.C. 450b(3), many of which are located along the Nation's borders and in border states, have unique concerns to address with the Department, and have difficulty sharing and receiving important information from the Department. The Tribal Security Officer shall coordinate the flow of information and ensure that tribal concerns are appropriately considered in the development and implementation of Departmental policies and programs.

The Director of Cargo Security Policy will operate under the direction and control of the Under Secretary for Policy. The responsibilities of the Director will include: advising the Assistant Secretary for Policy regarding all Departmental cargo security programs, policies, and initiatives; developing Department-wide cargo security policies; and coordinating Departmental cargo security policies and programs with other Federal departments and agencies. The Director's coordination role includes working with officials of the Departments of Energy and State in the negotiation of international cargo security agreements.

TITLE IV—OFFICE OF DOMESTIC NUCLEAR DETECTION

Section 401. Establishment of Office

Section 2001—Domestic Nuclear Detection Office

This section establishes the Domestic Nuclear Detection Office (DNDO) within the Department of Homeland Security, which shall be administered by a Director, who shall be appointed by the President. The DNDO will be focused on detecting and preventing the unauthorized importation, possession, storage, transportation, development, or use of a nuclear explosive device, fissile material, or radiological material against the United States.

The Committee strongly supports the establishment of the Domestic Nuclear Detection Office. Should terrorists gain access to the requisite material for a nuclear explosive, it is essential that we develop and utilize the best possible technology to assist interdiction prior to attack. Detection technologies, particularly when combined with timely intelligence, can be vitally important in this regard.

Section 2002—Functions of the Director of the Domestic Nuclear Detection Office

This section directs the Secretary of Homeland Security to vest in the Director of the Domestic Nuclear Detection Office (DNDO) the primary responsibility for implementing the Department's programs related to the detection and prevention of nuclear and radiological terrorism. The Director is also responsible for coordinating

such programs with other Federal agencies performing related activities.

The authority to administer all of the Department's research and development as well as acquisition and deployment programs for nuclear and radiological detection systems that had previously existed in other elements of the Department is transferred to DNDO. This includes the Department of Energy's Nuclear Assessment Program and the Environmental Measurements Laboratory which were transferred to the Department in 2002. Section 2010(c) provides for the transfer of relevant nuclear and radiological programs that were previously in the Science and Technology Directorate to DNDO.

Section 2003—Global Nuclear Detection Architecture

This section requires the Director of the Domestic Nuclear Detection Office to develop a global strategy for interdicting illicit nuclear and radiological material. This strategy will be used to guide detector deployments under the "global nuclear detection architecture." The architecture is a multi-layered system of detectors deployed internationally and domestically to detect and interdict nuclear materials intended for illicit use. The Director is assigned the responsibility of implementing the architecture within U.S. borders. The Department of Energy, Department of State, the Department of Defense, and others will continue to implement foreign deployments as part of their missions, but the Director has the authority to perform such deployments as necessary. The Director must ensure that the efforts of all participants are coordinated in order to create a fully integrated detection system.

Section 2004—Research and development

This section requires the Director of the Domestic Nuclear Detection Office to develop and execute a research and development program focused on achieving dramatically improved detection capabilities for nuclear explosive devices as well as radiological dispersion devices. This requirement recognizes and attempts to correct the current deficiencies in radiation detection technologies. This section promotes "transformational" research and development by requiring support for high-risk as well as long term projects. As other Federal agencies are engaged in radiation detection research there is a requirement for coordination to avoid duplication and encourage technology sharing. This should allow for more strategic investments across the Federal government.

Section 2005—System assessments

This section requires the technology development and acquisition programs within the Domestic Nuclear Detection Office (DNDO) to make use of a rigorous testing program to provide a "bottom line" assessment of capabilities prior to deployment. Problems have existed in the past where technologies have been acquired and deployed without knowledge of their true capabilities. The required testing will ensure that performance capabilities under realistic operating conditions will be known. For newly developed, advanced detection systems, it will also enable the verification that desired capabilities have been attained.

The design of the global detection architecture will also be evaluated. This evaluation will look at the effectiveness of the system of detectors as a whole, rather than individual detectors. Red teaming activities will be used to develop an understanding of possible adversary strategies and concealment methods. Net assessments can then gauge the overall system performance against these tactics. Results will be used to optimize detection system deployment and to guide the research programs within the Office.

Section 2006—Technology acquisition, deployment, support and training

This section authorizes the Domestic Nuclear Detection Office (DNDO) to purchase the requisite detection systems to implement the domestic portion of the detection architecture as well as any foreign deployments. The Director will acquire such systems for all of the Department's operational units that require them, including Customs and Border Protection. The Director will make recommendations to the Undersecretary for Science and Technology as to whether the acquired detection systems fulfill the existing criteria for protection under the SAFETY Act , Subtitle G of title VIII of the Homeland Security Act of 2002 (P.L. 107–296).

As systems are deployed, a key element of their effectiveness will be competent operational support. The Director is required to provide training to end users to ensure that the systems will be operated properly. Technical reachback, assistance by technical experts in interpreting detector data, is critical and must also be provided. Alarms must be reviewed to determine if they are valid or they result from a benign source of radiation or detector malfunction.

Section 2007—Situational awareness

The Director of the Domestic Nuclear Detection Office (DNDO) is made responsible for monitoring the global network of detection systems for valid alarms. Should an alarm be verified as an actual smuggling event, the Director must immediately inform the relevant response entities of the Federal government. The DNDO must also be ready to assist in resolving alarms or incidents reported by any Federal, State, tribal or local officials.

It will be important for the DNDO to gather and archive the data from the routine operation of its detection systems. This information can be used to better characterize the radiation signatures associated with benign flows of commerce and understand the impact of naturally occurring radioactive material. This knowledge can then be used to strengthen the effectiveness of the global architecture in detecting illicit nuclear and radiological material.

Section 2008—Forensic analysis

The Domestic Nuclear Detection Office (DNDO) is given the authority in this section to implement the Department of Homeland Security (DHS) programs as necessary to develop the analytical capabilities required to determine the nature of any seized nuclear or radiological material and its likely source. Through its Nuclear Assessment Program, the DNDO is already engaged in investigating nuclear smuggling events.

Section 2009—Threat information

This section gives the Director of the Domestic Nuclear Detection Office (DNDO) access, through the Secretary of Homeland Security, to all information, including intelligence, necessary to successfully fulfill the Director's responsibilities. The Director will also request the necessary analytic support from the Chief Intelligence Officer. The Director is authorized to hire professional analysts to perform the requisite work within the Office. The Director will submit intelligence collection requests through the Chief Intelligence Officer as needed.

All aspects of the Director's functions must be informed with the best available intelligence information. The design and implementation of an effective global detection architecture requires strategic placement of detectors. Such decisions must be informed, and require insight into known smuggling routes, global locations of nuclear material, and known terrorist tactics. Similarly, the detection signatures of various nuclear and radiological devices and materials must be identified to support research and development efforts and to test detection systems.

Section 2010—Administrative authorities

This section gives the Director of the Domestic Nuclear Detection Office (DNDO) the same hiring authorities as the Homeland Security Advanced Research Projects Agency (HSARPA) which are designed to attract highly qualified technical personnel.

Section 2011—Report requirement

This section requires the Director of the Domestic Nuclear Detection Office to submit to the appropriate Congressional committees an annual report containing the following information: the global detection strategy developed under section 2003 the status of implementation of such architecture, the schedule for future detection system deployments under such architecture, the research and development program of the Office, and a summary of actions taken by the Office during the reporting period to counter nuclear and radiological threats. This will give the congress the information it needs to review budgets and evaluate progress.

Section 2012—Advisory council on nuclear detection

The Director of the Domestic Nuclear Detection Office (DNDO) shall form a five member advisory council on nuclear detection which will, at the request of the Director, provide advice on the design of the global detection architecture and the DNDO research and development program. The Council will be made up of non-governmental experts on nuclear detection and related topics. The Secretary of Homeland Security is authorized under Section 871 of the Homeland Security Act of 2002 (P.L. 107–296) to exempt the Council from requirements under the Federal Advisory Committee Act (Public Law 92–463). The Committee believes such an exemption would be appropriate for this Council given the sensitive nature of its mission.

Section 2013—Interagency coordination council

This section requires the Director of the Domestic Nuclear Detection Office (DNDO) to coordinate the implementation of the global

nuclear detection architecture and the DNDO research and development program with other relevant Federal agencies. Through its Container Security Initiative, the Department of Homeland Security oversees the examination of high risk cargo in foreign ports. However, other Federal agencies, such as the Department of Energy and the Department of Defense, have been engaged in complementary activities in many countries and perform related detection research and development. The Director will chair an interagency coordination council to be established by the President. The President will direct representatives from all relevant agencies to join the interagency council to ensure that the work of each agency contributes to the deployment of an effective and efficient global detection architecture. The precise operation of the council is left for the President to determine.

Section 2014—Authorization of appropriations

This section authorizes the full budget request of $536 million for the Domestic Nuclear Detection Office (DNDO) to perform its duties in Fiscal Year 2007 and such sums as necessary for each subsequent fiscal year. This funding is sufficient to support the full spectrum of activities described in this title.

Section 2015—Definitions

The section contains the definitions of the terms used in this title. It also contains necessary conforming and clerical amendments.

This section defines "nuclear and radiological detection systems" as any technology "capable of detecting or identifying nuclear and radiological material or explosive devices." This definition focuses on the matter to be detected and not the means of detection. This is done to provide the widest possible latitude in the selection of detection technology.

Section 402. Nuclear and radiological detection systems

This section will promote the development of next generation, radiation detection capabilities and make this capability available at high volume seaports where it is most needed. As the Fiscal Year 2007 Domestic Nuclear Detection Office (DNDO) budget includes funds for the requisite number of deployments, additional funds should not be needed to implement this section.

This section requires nuclear and radiological detection capabilities to be deployed at 22 United States seaports by the end of Fiscal Year 2007. If selected on a basis of volume, the 22 seaports would represent sites where 98 percent of all containerized cargo enters the United States. A report shall be submitted to Congress within 90 days of enactment describing the risk-based prioritization of U.S. seaports used to guide nuclear and radiological detection system deployment. The timeline of deployment, type of systems, standard operating procedures and policy for use of such system shall be included in the report. Classified annexes will be included that describe any plans for covert testing of the systems and the risk based approach utilized to identify the priority seaports. Within 180 days of enactment, a safety plan shall also be submitted to Congress which describes the potential health and safety risks in using any of these systems.

This section requires the pilot deployment and operational testing of next generation radiation portal monitor (RPM) technology at one or more seaports by January 1, 2007, and if the desired level of performance is attained after 3 months of testing, it requires DNDO to make the advanced capability available to all high volume, U.S. seaports before September 30, 2007. (Next generation RPMs possess radioisotope identification capabilities.) The Director of DNDO shall report to Congress the results of the pilot testing program and any implementation problems with the subsequent deployments. Should such deployments be judged to be inefficient or wasteful, e.g., the benefits of the next-generation technology are insufficient or do not outweigh the costs when compared to existing systems, the Secretary shall notify Congress and recommend alternative actions.

The nature of operations at high volume seaports limits the effectiveness and feasibility of operation of current generation radiation portal monitors (RPMs). As current RPMs detect any radiation, they will alarm when a naturally occurring radiation source is in a container, e.g., bananas. These so-called "nuisance alarms" can be intolerable at large volume seaports, leading operators to turn down the sensitivity of the RPM, essentially rendering them useless. Next generation RPMs will be capable of measuring the energy of the radiation emitted, so they can distinguish a benign radiation source from actual threats. Nuisance alarm rates should therefore be dramatically reduced. When proven effective, they will enable a much larger fraction of cargo to be examined without slowing the flow of commerce.

The section does not require 100 percent screening of containerized cargo at these seaports. In fact it does not specify any cargo screening quota. Decisions to screen will still be based on a risk based approach. It does require that better screening capabilities, when proven, be made widely available. The proven technology will be available for foreign deployment as well. The reduction in nuisance alarms may ease concerns of foreign port operators over disruptions in operations.

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):

CHAPTER 701 OF TITLE 46, UNITED STATES CODE

CHAPTER 701—PORT SECURITY

Sec.
70101. Definitions.

* * * * * * *

[70107. Grants.]

* * * * * * *

70122. Maritime security command centers.

§ 70101. Definitions

For the purpose of this chapter:

(1) * * *

* * * * * * *

(6) The term "transportation security incident" means a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption *(other than economic disruption caused by acts that are unrelated to terrorism and are committed during a labor strike, demonstration, or other type of labor unrest)* in a particular area.

* * * * * * *

§ 70103. Maritime transportation security plans

(a) NATIONAL MARITIME TRANSPORTATION SECURITY PLAN.—(1) * * *

(2) The National Maritime Transportation Security Plan shall provide for efficient, coordinated, and effective action to deter and minimize damage from a transportation security incident, and shall include the following:

(A) * * *

* * * * * * *

(J)*(i)* A plan for ensuring that the flow of cargo through United States ports is reestablished as efficiently and quickly as possible after a transportation security incident.

(ii) The plan required by clause (i) shall include protocols for the resumption of trade in the event of a transportation security incident that necessitates the suspension of trade through contingency and continuity planning that ensures trade lanes are restored as quickly as possible. The protocols shall provide for—

(I) coordination with appropriate Federal, State, and local agencies, the private sector, and appropriate overseas entities in developing such contingency and continuity planning;

(II) coordination with appropriate Federal, State, and local agencies and the private sector on law enforcement actions, inter-modal rerouting plans, and identification and prioritization of goods that may enter the United States; and

(III) designation of appropriate Federal officials to work with port authorities to reestablish the flow of cargo by prioritizing shipments based on appropriate factors, including factors relating to public health, national security, and economic need.

* * * * * * *

(c) VESSEL AND FACILITY SECURITY PLANS.—(1) * * *

* * * * * * *

(3) A security plan required under this subsection shall—

(A) * * *

* * * * * * *

(C) include provisions for—

(i) * * *

(ii) establishing and controlling access to secure areas of the vessel or facility*, including access by individuals en-*

gaged in the surface transportation of intermodal containers in or out of a port facility;

* * * * * * *

(E) describe [the training, periodic unannounced drills, and] security actions of persons on the vessel or at the facility, to be carried out under the plan to deter to the maximum extent practicable a transportation security incident, or a substantial threat of such a security incident;

(F) provide a strategy and timeline for conducting training and periodic unannounced drills for persons on the vessel or at the facility to be carried out under the plan to deter, to the maximum extent practicable, a transportation security incident or a substantial threat of such a transportation security incident;

[(F)] *(G)* be updated at least every 5 years; and

[(G)] *(H)* be resubmitted for approval of each change to the vessel or facility that may substantially affect the security of the vessel or facility.

(4) The Secretary shall—

(A) * * *

* * * * * * *

[(D) review each plan periodically thereafter.]

(D) verify the effectiveness of each such facility security plan periodically, but not less than twice annually, at least one of which shall be an inspection of the facility that is conducted without notice to the facility.

* * * * * * *

§ 70105. Transportation security cards

(a) * * *

* * * * * * *

(c) DETERMINATION OF TERRORISM SECURITY RISK.—(1) * * *

(2) The Secretary shall prescribe regulations that establish a waiver process for issuing a transportation security card to an individual found to be otherwise ineligible for such a card under *subparagraph (A), (B), or (D) of* paragraph (1). In deciding to issue a card to such an individual, the Secretary shall—

(A) * * *

* * * * * * *

[§ 70107. Grants

[(a) IN GENERAL.—The Secretary shall establish a grant program for making a fair and equitable allocation of funds to implement Area Maritime Transportation Security Plans and facility security plans among port authorities, facility operators, and State and local government agencies required to provide port security services. Before awarding a grant under the program, the Secretary shall provide for review and comment by the appropriate Federal Maritime Security Coordinators and the Maritime Administrator. In administering the grant program, the Secretary shall take into account national economic and strategic defense concerns.

[(b) ELIGIBLE COSTS.—The following costs of funding the correction of Coast Guard identified vulnerabilities in port security and

ensuring compliance with Area Maritime Transportation Security Plans and facility security plans are eligible to be funded:

[(1) Salary, benefits, overtime compensation, retirement contributions, and other costs of additional Coast Guard mandated security personnel.

[(2) The cost of acquisition, operation, and maintenance of security equipment or facilities to be used for security monitoring and recording, security gates and fencing, marine barriers for designated security zones, security-related lighting systems, remote surveillance, concealed video systems, security vessels, and other security-related infrastructure or equipment that contributes to the overall security of passengers, cargo, or crewmembers.

[(3) The cost of screening equipment, including equipment that detects weapons of mass destruction and conventional explosives, and of testing and evaluating such equipment, to certify secure systems of transportation.

[(4) The cost of conducting vulnerability assessments to evaluate and make recommendations with respect to security.

[(c) MATCHING REQUIREMENTS.—

[(1) 75-PERCENT FEDERAL FUNDING.—Except as provided in paragraph (2), Federal funds for any eligible project under this section shall not exceed 75 percent of the total cost of such project.

[(2) EXCEPTIONS.—

[(A) SMALL PROJECTS.—There are no matching requirements for grants under subsection (a) for projects costing not more than $25,000.

[(B) HIGHER LEVEL OF SUPPORT REQUIRED.—If the Secretary determines that a proposed project merits support and cannot be undertaken without a higher rate of Federal support, then the Secretary may approve grants under this section with a matching requirement other than that specified in paragraph (1).

[(d) COORDINATION AND COOPERATION AGREEMENTS.—The Secretary shall ensure that projects paid for, or the costs of which are reimbursed, under this section within any area or port are coordinated with other projects, and may require cooperative agreements among users of the port and port facilities with respect to projects funded under this section.

[(e) ADMINISTRATION.—

[(1) IN GENERAL.—The program shall require eligible port authorities, facility operators, and State and local agencies required to provide security services, to submit an application, at such time, in such form, and containing such information and assurances as the Secretary may require, and shall include appropriate application, review, and delivery mechanisms.

[(2) MINIMUM STANDARDS FOR PAYMENT OR REIMBURSEMENT.—Each application for payment or reimbursement of eligible costs shall include, at a minimum, the following:

[(A) A copy of the applicable Area Maritime Transportation Security Plan or facility security plan.

[(B) A comprehensive description of the need for the project, and a statement of the project's relationship to the

applicable Area Maritime Transportation Security Plan or facility security plan.

[(C) A determination by the Captain of the Port that the security project addresses or corrects Coast Guard identified vulnerabilities in security and ensures compliance with Area Maritime Transportation Security Plans and facility security plans.

[(3) PROCEDURAL SAFEGUARDS.—The Secretary shall by regulation establish appropriate accounting, reporting, and review procedures to ensure that amounts paid or reimbursed under this section are used for the purposes for which they were made available, all expenditures are properly accounted for, and amounts not used for such purposes and amounts not obligated or expended are recovered.

[(4) PROJECT APPROVAL REQUIRED.—The Secretary may approve an application for the payment or reimbursement of costs under this section only if the Secretary is satisfied that—

[(A) the project is consistent with Coast Guard vulnerability assessments and ensures compliance with Area Maritime Transportation Security Plans and facility security plans;

[(B) enough money is available to pay the project costs that will not be reimbursed by the United States Government under this section;

[(C) the project will be completed without unreasonable delay; and

[(D) the recipient has authority to carry out the project as proposed.

[(f) AUDITS AND EXAMINATIONS.—A recipient of amounts made available under this section shall keep such records as the Secretary may require, and make them available for review and audit by the Secretary, the Comptroller General of the United States, or the Inspector General of the department in which the Coast Guard is operating.

[(g) REPORTS ON SECURITY FUNDING AND COMPLIANCE.—

[(1) INITIAL REPORT.—Within 6 months after the date of enactment of this Act, the Secretary shall transmit an unclassified report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Transportation and Infrastructure, that—

[(A) includes a funding proposal and rationale to fund the correction of Coast Guard identified vulnerabilities in port security and to help ensure compliance with Area Maritime Transportation Security Plans and facility security plans for fiscal years 2003 through 2008; and

[(B) includes projected funding proposals for fiscal years 2003 through 2008 for the following security programs:

[(i) The Sea Marshall program.

[(ii) The Automated Identification System and a system of polling vessels on entry into United States waters.

[(iii) The maritime intelligence requirements in this Act.

[(iv) The issuance of transportation security cards required by section 70105.

[(v) The program of certifying secure systems of transportation.

[(2) OTHER EXPENDITURES.—The Secretary shall, as part of the report required by paragraph (1) report, in coordination with the Commissioner of Customs, on projected expenditures of screening and detection equipment and on cargo security programs over fiscal years 2003 through 2008.

[(3) ANNUAL REPORTS.—Annually, beginning 1 year after transmittal of the report required by paragraph (1) until October 1, 2009, the Secretary shall transmit an unclassified annual report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Transportation and Infrastructure, on progress in achieving compliance with the correction of Coast Guard identified vulnerabilities in port security and compliance with Area Maritime Transportation Security Plans and facility security plans that—

[(A) identifies any modifications necessary in funding to ensure the correction of Coast Guard identified vulnerabilities and ensure compliance with Area Maritime Transportation Security Plans and facility security plans;

[(B) includes an assessment of progress in implementing the grant program established by subsection (a);

[(C) includes any recommendations the Secretary may make to improve these programs; and

[(D) with respect to a port selected by the Secretary, describes progress and enhancements of applicable Area Maritime Transportation Security Plans and facility security plans and how the Maritime Transportation Security Act of 2002 has improved security at that port.

[(h) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary for each of fiscal years 2003 through 2008 such sums as are necessary to carry out subsections (a) through (g).

[(i) INVESTIGATIONS.—

[(1) IN GENERAL.—The Secretary shall conduct investigations, fund pilot programs, and award grants, to examine or develop—

[(A) methods or programs to increase the ability to target for inspection vessels, cargo, crewmembers, or passengers that will arrive or have arrived at any port or place in the United States;

[(B) equipment to detect accurately explosives, chemical, or biological agents that could be used in a transportation security incident against the United States;

[(C) equipment to detect accurately nuclear or radiological materials, including scintillation-based detection equipment capable of signalling the presence of nuclear or radiological materials;

[(D) improved tags and seals designed for use on shipping containers to track the transportation of the merchandise in such containers, including sensors that are able to track a container throughout its entire supply chain, detect hazardous and radioactive materials within that con-

tainer, and transmit that information to the appropriate law enforcement authorities;

[(E) tools, including the use of satellite tracking systems, to increase the awareness of maritime areas and to identify potential transportation security incidents that could have an impact on facilities, vessels, and infrastructure on or adjacent to navigable waterways, including underwater access;

[(F) tools to mitigate the consequences of a transportation security incident on, adjacent to, or under navigable waters of the United States, including sensor equipment, and other tools to help coordinate effective response to a transportation security incident;

[(G) applications to apply existing technologies from other areas or industries to increase overall port security;

[(H) improved container design, including blast-resistant containers; and

[(I) methods to improve security and sustainability of port facilities in the event of a maritime transportation security incident, including specialized inspection facilities.

[(2) IMPLEMENTATION OF TECHNOLOGY.—

[(A) IN GENERAL.—In conjunction with ongoing efforts to improve security at United States ports, the Secretary may conduct pilot projects at United States ports to test the effectiveness and applicability of new port security projects, including—

[(i) testing of new detection and screening technologies;

[(ii) projects to protect United States ports and infrastructure on or adjacent to the navigable waters of the United States, including underwater access; and

[(iii) tools for responding to a transportation security incident at United States ports and infrastructure on or adjacent to the navigable waters of the United States, including underwater access.

[(B) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Secretary $35,000,000 for each of fiscal years 2005 through 2009 to carry out this subsection.

[(3) NATIONAL PORT SECURITY CENTERS.—

[(A) IN GENERAL.—The Secretary may make grants or enter into cooperative agreements with eligible nonprofit institutions of higher learning to conduct investigations in collaboration with ports and the maritime transportation industry focused on enhancing security of the Nation's ports in accordance with this subsection through National Port Security Centers.

[(B) APPLICATIONS.—To be eligible to receive a grant under this paragraph, a nonprofit institution of higher learning, or a consortium of such institutions, shall submit an application to the Secretary in such form and containing such information as the Secretary may require.

[(C) COMPETITIVE SELECTION PROCESS.—The Secretary shall select grant recipients under this paragraph through a competitive process on the basis of the following criteria:

[(i) Whether the applicant can demonstrate that personnel, laboratory, and organizational resources will be available to the applicant to carry out the investigations authorized in this paragraph.

[(ii) The applicant's capability to provide leadership in making national and regional contributions to the solution of immediate and long-range port and maritime transportation security and risk mitigation problems.

[(iii) Whether the applicant can demonstrate that is has an established, nationally recognized program in disciplines that contribute directly to maritime transportation safety and education.

[(iv) Whether the applicant's investigations will involve major United States ports on the East Coast, the Gulf Coast, and the West Coast, and Federal agencies and other entities with expertise in port and maritime transportation.

[(v) Whether the applicant has a strategic plan for carrying out the proposed investigations under the grant.

[(4) ADMINISTRATIVE PROVISIONS.—

[(A) NO DUPLICATION OF EFFORT.—Before making any grant, the Secretary shall coordinate with other Federal agencies to ensure the grant will not duplicate work already being conducted with Federal funding.

[(B) ACCOUNTING.—The Secretary shall by regulation establish accounting, reporting, and review procedures to ensure that funds made available under paragraph (1) are used for the purpose for which they were made available, that all expenditures are properly accounted for, and that amounts not used for such purposes and amounts not expended are recovered.

[(C) RECORDKEEPING.—Recipients of grants shall keep all records related to expenditures and obligations of funds provided under paragraph (1) and make them available upon request to the Inspector General of the department in which the Coast Guard is operating and the Secretary for audit and examination.

[(5) ANNUAL REVIEW AND REPORT.—The Inspector General of the department in which the Coast Guard is operating shall annually review the programs established under this subsection to ensure that the expenditures and obligations of funds are consistent with the purposes for which they are provided, and report the findings to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure of the House of Representatives.]

§ 70108. Foreign port assessment

(a) * * *

* * * * * * *

(d) PERIODIC REASSESSMENT.—The Secretary, acting through the Commandant of the Coast Guard, shall reassess the effectiveness of antiterrorism measures maintained at ports as described under sub-

section (a) and of procedures described in subsection (b) not less than every 3 years.

* * * * * * *

§ 70115. Long-range vessel tracking system

[The Secretary**]** *Not later than April 1, 2007, the Secretary* shall, consistent with international treaties, conventions, and agreements to which the United States is a party, develop and implement a long-range automated vessel tracking system for all vessels in United States waters that are equipped with the Global Maritime Distress and Safety System or equivalent satellite technology. The system shall be designed to provide the Secretary the capability of receiving information on vessel positions at interval positions appropriate to deter transportation security incidents. The Secretary may use existing maritime organizations to collect and monitor tracking information under the system.

* * * * * * *

§ 70122. Maritime security command centers

(a) ESTABLISHMENT.—The Secretary shall establish an integrated network of virtual and physical maritime security command centers at appropriate United States seaports and maritime regions, as determined by the Secretary, to—

(1) enhance information sharing;

(2) facilitate day-to-day operational coordination; and

(3) in the case of a transportation security incident, facilitate incident management and response.

(b) CHARACTERISTICS.—Each maritime security command center described in subsection (a) shall—

(1) be regionally based and utilize where available the compositional and operational characteristics, facilities and information technology systems of current operational centers for port and maritime security and other similar existing facilities and systems;

(2) be adapted to meet the security needs, requirements, and resources of the seaport and maritime region the center will cover; and

(3) to the maximum extent practicable, not involve the construction of new facilities, but shall utilize information technology, virtual connectivity, and existing facilities to create an integrated, real-time communication and information sharing network.

(c) PARTICIPATION.—The following entities shall participate in the integrated network of maritime security command centers described in subsection (a):

(1) The Coast Guard.

(2) U.S. Customs and Border Protection.

(3) U.S. Immigration and Customs Enforcement.

(4) Other appropriate Federal, State, and local law enforcement agencies.

(d) RESPONSIBILITIES.—Each maritime security command center described in subsection (a) shall—

(1) assist, as appropriate, in the implementation of maritime transportation security plans developed under section 70103;

(2) implement the transportation security incident response plans required under section 70104;

(3) carry out information sharing activities consistent with those activities required under section 1016 of the National Security Intelligence Reform Act of 2004 (6 U.S.C. 485) and the Homeland Security Information Sharing Act (6 U.S.C. 481 et seq.);

(4) conduct short- and long-range vessel tracking under sections 70114 and 70115; and

(5) carry out such other responsibilities as determined by the Secretary.

(e) SECURITY CLEARANCES.—The Secretary shall sponsor and expedite individuals participating in a maritime security command center described in subsection (a) in gaining or maintaining their security clearances. Through the Captain of the Port, the Secretary may identify key individuals who should participate. In addition, the port or other entities may appeal to the Captain of the Port for sponsorship.

(f) SECURITY INCIDENTS.—During a transportation security incident involving the port, the Coast Guard Captain of the Port designated by the Commandant of the Coast Guard in a maritime security command center described in subsection (a) shall act as the incident commander, unless otherwise directed by the President.

(g) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to affect the normal command and control procedures for operational entities in the Department, unless so directed by the Secretary.

(h) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated $60,000,000 for each of the fiscal years 2007 through 2012 to carry out this section and section 108(c) of the Security and Accountability For Every Port Act.

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

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

Sec. 1. Short title; table of contents.

* * * * * * *

TITLE V—EMERGENCY PREPAREDNESS AND RESPONSE

Sec. 501. Under Secretary for Emergency Preparedness and Response.

* * * * * * *

Sec. 510. Procurement of security countermeasures for strategic national stockpile.
Sec. 511. Urban and other high risk area communications capabilities.
Sec. 512. Port security grant program.

[TITLE VI—TREATMENT OF CHARITABLE TRUSTS FOR MEMBERS OF THE ARMED FORCES OF THE UNITED STATES AND OTHER GOVERNMENTAL ORGANIZATIONS

[Sec. 601. Treatment of charitable trusts for members of the Armed Forces of the United States and other governmental organizations.]

TITLE VI—POLICY, PLANNING, AND INTERNATIONAL AFFAIRS

Sec. 601. Directorate for Policy, Planning, and International Affairs.

Sec. 602. Office of International Affairs.
Sec. 603. Other offices and officials.

* * * * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

Subtitle A—Coordination with Non-Federal Entities

Sec. 801. Office for State and Local Government Coordination.
Sec. 802. Port security training program.
Sec. 803. Port security exercise program.

* * * * * * *

Subtitle H—Miscellaneous Provisions

* * * * * * *

[Sec. 879. Office of International Affairs.]

* * * * * * *

TITLE XVIII—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN

Subtitle A—General Provisions

Sec. 1801. Strategic plan to enhance the security of the international supply chain.
Sec. 1802. Transmission of additional data elements for improved high risk targeting.
Sec. 1803. Plan to improve the Automated Targeting System.
Sec. 1804. Container standards and verification procedures.
Sec. 1805. Container Security Initiative (CSI).
Sec. 1806. Information sharing relating to supply chain security cooperation.

Subtitle B—Customs-Trade Partnership Against Terrorism (C-TPAT)

Sec. 1811. Establishment.
Sec. 1812. Eligible entities.
Sec. 1813. Minimum requirements.
Sec. 1814. Tier one participants.
Sec. 1815. Tier two participants.
Sec. 1816. Tier three participants.
Sec. 1817. Consequences for lack of compliance.
Sec. 1818. Validations by third party entities.
Sec. 1819. Revalidation.
Sec. 1820. Non-containerized cargo.
Sec. 1821. Authorization of appropriations.

Subtitle C—Miscellaneous Provisions

Sec. 1831. Research, development, test, and evaluation efforts in furtherance of maritime and cargo security.
Sec. 1832. Grants under Operation Safe Commerce.
Sec. 1833. Definitions.

TITLE XIX—MISCELLANEOUS PROVISIONS

Sec. 1901. Treatment of charitable trusts for members of the armed forces of the United States and other governmental organizations.

TITLE XX—OFFICE OF DOMESTIC NUCLEAR DETECTION

Sec. 2001. Domestic Nuclear Detection Office.
Sec. 2002. Functions of Director of the Domestic Nuclear Detection Office, generally.
Sec. 2003. Global nuclear detection architecture.
Sec. 2004. Research and development.
Sec. 2005. System assessments.
Sec. 2006. Technology acquisition, deployment, support, and training.
Sec. 2007. Situational awareness.
Sec. 2008. Forensic analysis.
Sec. 2009. Threat information.
Sec. 2010. Administrative authorities.
Sec. 2011. Report requirement.
Sec. 2012. Advisory Council on Nuclear Detection.

Sec. 2013. Interagency coordination council.
Sec. 2014. Authorization of appropriations.
Sec. 2015. Definitions.

* * * * * * *

TITLE I—DEPARTMENT OF HOMELAND SECURITY

* * * * * * *

SEC. 103. OTHER OFFICERS.

(a) * * *

* * * * * * *

(d) OTHER OFFICERS.—To assist the Secretary in the performance of the Secretary's functions, there are the following officers, appointed by the President:

(1) * * *

* * * * * * *

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

* * * * * * *

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

SEC. 302. RESPONSIBILITIES AND AUTHORITIES OF THE UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY.

The Secretary, acting through the Under Secretary for Science and Technology, shall have the responsibility for—

(1) * * *

(2) developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for, identifying priorities, goals, objectives and policies for, and coordinating the Federal Government's civilian efforts to identify and develop countermeasures to chemical, biological, [radiological, nuclear,] and other emerging terrorist threats, including the development of comprehensive, research-based definable goals for such efforts and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts;

* * * * * * *

(5) establishing priorities for, directing, funding, and conducting national research, development, test and evaluation, and procurement of technology and systems for—

(A) preventing the importation of chemical, biological, [radiological, nuclear,] and related weapons and material; and

* * * * * * *

SEC. 305. FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTERS.

The Secretary, acting through the Under Secretary for Science and Technology *and the Director of the Domestic Nuclear Detection Office*, shall have the authority to establish or contract with 1 or more federally funded research and development centers to provide independent analysis of homeland security issues, or to carry out other responsibilities under this Act, including coordinating and integrating both the extramural and intramural programs described in section 308.

* * * * * * *

SEC. 308. CONDUCT OF RESEARCH, DEVELOPMENT, DEMONSTRATION, TESTING AND EVALUATION.

(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology *and the Director of the Domestic Nuclear Detection Office*, shall carry out the responsibilities under section 302(4) through both extramural and intramural programs.

(b) EXTRAMURAL PROGRAMS.—

(1) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology *and the Director of the Domestic Nuclear Detection Office*, shall operate extramural research, development, demonstration, testing, and evaluation programs so as to—

(A) * * *

* * * * * * *

TITLE V—EMERGENCY PREPAREDNESS AND RESPONSE

* * * * * * *

SEC. [510] *511*. URBAN AND OTHER HIGH RISK AREA COMMUNICATIONS CAPABILITIES.

(a) * * *

* * * * * * *

SEC. 512. PORT SECURITY GRANT PROGRAM.

(a) GRANTS AUTHORIZED.—The Secretary shall establish a grant program to allocate Federal financial assistance to United States seaports on the basis of risk and need.

(b) PRIORITIZATION PROCESS.—In awarding grants under this section, the Secretary shall conduct an assessment of United States seaports to develop a prioritization for awarding grants authorized under subsection (a) based upon—

(1) the most current risk assessment available from the Department;

(2) the national economic and strategic defense considerations of individual ports; and

(3) any other factors that the Secretary determines to be appropriate.

(c) APPLICATION.—

(1) IN GENERAL.—Any entity or facility subject to an Area Maritime Transportation Security Plan required under subsection (b) or (c) of section 70103 of title 46, United States Code,

may submit an application for a grant under this section, at such time, in such form, and containing such information and assurances as the Secretary may require.

(2) MINIMUM STANDARDS FOR PAYMENT OR REIMBURSEMENT.—Each application submitted under paragraph (1) shall include—

(A) a comprehensive description of—

(i) the purpose of the project for which the applicant seeks a grant under this section and why the applicant needs the grant;

(ii) the applicability of the project to the Area Maritime Transportation Security Plan and other homeland security plans;

(iii) the methodology for coordinating the project into the security of the greater port area, as identified in the Area Maritime Transportation Security Plan;

(iv) any existing cooperation or mutual aid agreements with other port facilities, vessels, organizations, or State, territorial, and local governments as such agreements relate to port security; and

(v) a capital budget showing how the applicant intends to allocate and expend the grant funds;

(B) a determination by the Captain of the Port that the project—

(i) addresses or corrects port security vulnerabilities; and

(ii) helps to ensure compliance with the Area Maritime Transportation Security Plan.

(3) PROCEDURAL SAFEGUARDS.—The Secretary, in consultation with the Office of the Inspector General and the Office of Grants and Training, shall issue guidelines to establish appropriate accounting, reporting, and review procedures to ensure that—

(A) grant funds are used for the purposes for which they were made available;

(B) grantees have properly accounted for all expenditures of grant funds; and

(C) grant funds not used for such purposes and amounts not obligated or expended are returned.

(d) USE OF FUNDS.—Grants awarded under this section may be used—

(1) to help implement Area Maritime Transportation Security Plans required under section 70103(b) of title 46, United States Code;

(2) to remedy port security vulnerabilities identified through vulnerability assessments approved by the Secretary;

(3) for non-Federal projects contributing to the overall security of a seaport or a system of United States seaports, as determined by the Secretary;

(4) for the salaries, benefits, overtime compensation, and other costs of additional security personnel for State and local agencies for activities required by the Area Maritime Transportation Security Plan for a seaport area if the Secretary—

(A) increases the threat level under the Homeland Security Advisory System to Code Orange or Code Red; or

(B) raises the Maritime Security level to MARSEC Level 2 or 3;

(5) for the cost of acquisition, operation, and maintenance of equipment that contributes to the overall security of the port area, as identified in the Area Maritime Transportation Security Plan, if the need is based upon vulnerability assessments approved by the Secretary or identified in the Area Maritime Security Plan;

(6) to conduct vulnerability assessments approved by the Secretary;

(7) to purchase or upgrade equipment, including computer software, to enhance terrorism preparedness;

(8) to conduct exercises or training for prevention and detection of, preparedness for, response to, or recovery from terrorist attacks;

(9) to establish or enhance mechanisms for sharing terrorism threat information;

(10) for the cost of equipment (including software) required to receive, transmit, handle, and store classified information;

(11) for the protection of critical infrastructure against potential attack by the addition of barriers, fences, gates, and other such devices, except that the cost of such measures may not exceed the greater of—

(A) $1,000,000 per project; or

(B) such greater amount as may be approved by the Secretary, which may not exceed 10 percent of the total amount of the grant; and

(12) to conduct port-wide exercises to strengthen emergency preparedness of Federal, State, territorial, and local officials responsible for port security, including law enforcement personnel and firefighters and other first responders, in support of the Area Maritime Security Plan.

(e) PROHIBITED USES.—Grants awarded under this section may not be used to—

(1) supplant State or local funds for activities of the type described in subsection (d);

(2) construct buildings or other physical facilities;

(3) acquire land; or

(4) make any State or local government cost-sharing contribution.

(f) MATCHING REQUIREMENT.—

(1) IN GENERAL.—Except as provided in subparagraph (A) or (B) of paragraph (2), Federal funds for any eligible project under this section shall not exceed 75 percent of the total cost of such project.

(2) EXCEPTIONS.—

(A) SMALL PROJECTS.—The requirement of paragraph (1) shall not apply with respect to a project with a total cost of not more than $25,000.

(B) HIGHER LEVEL OF FEDERAL SUPPORT REQUIRED.—The requirement of paragraph (1) shall not apply with respect to a project if the Secretary determines that the project merits support and cannot be undertaken without a higher rate of Federal support than the rate described in paragraph (1).

(3) IN-KIND CONTRIBUTIONS.—Each recipient of a grant under this section may meet the requirement of paragraph (1) by making in-kind contributions of goods or services that are directly linked with the purpose for which the grant is made, as determined by the Secretary, including any necessary personnel expenses, contractor services, administrative costs, equipment, fuel, or maintenance, and rental space.

(g) MULTIPLE PHASE PROJECTS.—

(1) IN GENERAL.—The Secretary may award grants under this section for projects that span multiple years.

(2) FUNDING LIMITATION.—Not more than 20 percent of the total grant funds awarded under this section in any fiscal year may be awarded for projects that span multiple years.

(h) CONSISTENCY WITH PLANS.—The Secretary shall ensure that each grant awarded under this section—

(1) is used to supplement and support, in a consistent and coordinated manner, the applicable Area Maritime Transportation Security Plan; and

(2) is coordinated with any applicable State or Urban Area Homeland Security Plan.

(i) COORDINATION AND COOPERATION.—The Secretary—

(1) shall ensure that all projects that receive grant funding under this section within any area defined in an Area Maritime Transportation Security Plan are coordinated with other projects in such area; and

(2) may require cooperative agreements among users of the seaport and seaport facilities with respect to projects funded under this section.

(j) REVIEW AND AUDITS.—The Secretary shall require all grantees under this section to maintain such records as the Secretary may require and make such records available for review and audit by the Secretary, the Comptroller General of the United States, or the Inspector General of the Department.

(k) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There are authorized to be appropriated $400,000,000 for each of fiscal years 2007 through 2012 to carry out this section.

(2) SOURCE OF FUNDS.—Amounts authorized to be appropriated under paragraph (1) shall originate from duties collected by U.S. Customs and Border Protection.

TITLE VI—POLICY, PLANNING, AND INTERNATIONAL AFFAIRS

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

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

(b) UNDER SECRETARY FOR POLICY.—

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

(2) QUALIFICATIONS.—No individual shall be appointed Under Secretary for Policy under paragraph (1) unless the indi-

vidual has, by education and experience, demonstrated knowledge, ability, and skill in the fields of policy and strategic planning.

(c) RESPONSIBILITIES OF UNDER SECRETARY.—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) the exchange of information on research and development on homeland security technologies;

(ii) joint training exercises of first responders in coordination with the Assistant Secretary for Grants and Training; and

(iii) exchanging expertise and information on terrorism prevention, response, and crisis management.

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

(C) To plan and participate in international conferences, exchange programs (including the exchange of scientists, engineers, and other experts), and other training activities with friendly nations

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

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

(F) To represent the Department in international negotiations, working groups, and standards-setting bodies.

(4) PRIVATE SECTOR.—

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

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

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

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

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

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

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

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

SEC. 602. OFFICE OF INTERNATIONAL AFFAIRS.

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

(b) DUTIES OF THE ASSISTANT SECRETARY.—The Assistant Secretary shall have the following duties:

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

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

(B) Joint training exercises of first responders.

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

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

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

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

SEC. 603. OTHER OFFICES AND OFFICIALS.

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

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

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

(A) a Secure Border Initiative Program Office; and

(B) a Screening Coordination and Operations Office.

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

(4) The Victim Assistance Officer.

(5) The Tribal Security Officer.

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

(b) DIRECTOR OF CARGO SECURITY POLICY.—

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

(2) RESPONSIBILITIES.—The Director shall—

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

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

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

* * * * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

Subtitle A—Coordination with Non-Federal Entities

* * * * * * *

SEC. 802. PORT SECURITY TRAINING PROGRAM.

(a) IN GENERAL.—The Secretary, acting through the Assistant Secretary for Grants and Training and in coordination with components of the Department with maritime security expertise, including the Coast Guard, the Transportation Security Administration, and U.S. Customs and Border Protection, shall establish a Port Security Training Program (hereinafter in this section referred to as the "Program") for the purpose of enhancing the capabilities of each of the Nation's commercial seaports to prevent, prepare for, respond to, mitigate against, and recover from threatened or actual acts of terrorism, natural disasters, and other emergencies.

(b) REQUIREMENTS.—The Program shall provide validated training that—

(1) reaches multiple disciplines, including Federal, State, and local government officials, commercial seaport personnel and management, and governmental and nongovernmental emergency response providers;

(2) provides training at the awareness, performance, and management and planning levels;

(3) utilizes multiple training mediums and methods, including—

(A) direct delivery;

(B) train-the-trainer;

(C) computer-based training;

(D) web-based training; and

(E) video teleconferencing;

(4) addresses port security topics, including—

(A) seaport security plans and procedures, including how security plans and procedures are adjusted when threat levels increase;

(B) seaport security force operations and management;

(C) physical security and access control at seaports;

(D) methods of security for preventing and countering cargo theft;

(E) container security;

(F) recognition and detection of weapons, dangerous substances, and devices;

(G) operation and maintenance of security equipment and systems;

(H) security threats and patterns;

(I) security incident procedures, including procedures for communicating with governmental and nongovernmental emergency response providers; and

(J) evacuation procedures;

(5) is consistent with, and supports implementation of, the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goal, and other such national initiatives;

(6) is evaluated against clear and consistent performance measures; and

(7) addresses security requirements under facility security plans.

(c) NATIONAL VOLUNTARY CONSENSUS STANDARDS.—The Secretary shall—

(1) support the development, promulgation, and regular updating as necessary of national voluntary consensus standards for port security training; and

(2) ensure that the training provided under this section is consistent with such standards.

(d) TRAINING PARTNERS.—In developing and delivering training under the Program, the Secretary shall—

(1) work with government training facilities, academic institutions, private organizations, employee organizations, and other entities that provide specialized, state-of-the-art training for governmental and nongovernmental emergency responder providers or commercial seaport personnel and management; and

(2) utilize, as appropriate, training courses provided by community colleges, public safety academies, State and private universities, and other facilities.

(e) CONSULTATION.—The Secretary shall ensure that, in carrying out the Program, the Office of Grants and Training shall consult with—

(1) a geographic and substantive cross section of governmental and nongovernmental emergency response providers; and

(2) commercial seaport personnel and management.

(f) COMMERCIAL SEAPORT PERSONNEL DEFINED.—For purposes of this section, the term "commercial seaport personnel" means any person engaged in an activity relating to the loading or unloading of cargo, the movement or tracking of cargo, the maintenance and repair of intermodal equipment, the operation of cargo-related equipment (whether or not integral to the vessel), and the handling of mooring lines on the dock when a vessel is made fast or let go, in the United States or the coastal waters thereof.

SEC. 803. PORT SECURITY EXERCISE PROGRAM.

(a) IN GENERAL.—The Secretary, acting through the Assistant Secretary for Grants and Training, shall establish a Port Security Exercise Program (hereinafter in this section referred to as the "Program") for the purpose of testing and evaluating the capabilities of Federal, State, local, and foreign governments, commercial seaport personnel and management, governmental and nongovernmental emergency response providers, the private sector, or any other organization or entity, as the Secretary determines to be appropriate, to

prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism, natural disasters, and other emergencies at commercial seaports.

(b) REQUIREMENTS.—The Secretary, acting through the Assistant Secretary for Grants and Training and in coordination with components of the Department with maritime security expertise, including the Coast Guard, the Transportation Security Administration, and U.S. Customs and Border Protection, shall ensure that the Program—

(1) consolidates all existing port security exercise programs administered by the Department;

(2) conducts, on a periodic basis, port security exercises at commercial seaports that are—

(A) scaled and tailored to the needs of each port;

(B) live in the case of the most at-risk ports;

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

(D) consistent with the National Incident Management System, the National Response Plan, the National Infrastructure Protection Plan, the National Preparedness Guidance, the National Preparedness Goal, and other such national initiatives;

(E) evaluated against clear and consistent performance measures;

(F) assessed to learn best practices, which shall be shared with appropriate Federal, State, and local officials, seaport personnel and management; governmental and nongovernmental emergency response providers, and the private sector; and

(G) followed by remedial action in response to lessons learned; and

(3) assists State and local governments and commercial seaports in designing, implementing, and evaluating exercises that—

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

(B) are consistent with any applicable Area Maritime Transportation Security Plan and State or Urban Area Homeland Security Plan.

(c) REMEDIAL ACTION MANAGEMENT SYSTEM.—The Secretary, acting through the Assistant Secretary for Grants and Training, shall establish a Remedial Action Management System to—

(1) identify and analyze each port security exercise for lessons learned and best practices;

(2) disseminate lessons learned and best practices to participants in the Program;

(3) monitor the implementation of lessons learned and best practices by participants in the Program; and

(4) conduct remedial action tracking and long-term trend analysis.

(d) GRANT PROGRAM FACTOR.—In evaluating and prioritizing applications for Federal financial assistance under section 512, the Secretary shall give additional consideration to those applicants that have conducted port security exercises under this section.

(e) CONSULTATION.—The Secretary shall ensure that, in carrying out the Program, the Office of Grants and Training shall consult with—

(1) a geographic and substantive cross section of governmental and nongovernmental emergency response providers; and

(2) commercial seaport personnel and management.

(f) COMMERCIAL SEAPORT PERSONNEL DEFINED.—For purposes of this section, the term "commercial seaport personnel" means any person engaged in an activity relating to the loading or unloading of cargo, the movement or tracking of cargo, the maintenance and repair of intermodal equipment, the operation of cargo-related equipment (whether or not integral to the vessel), and the handling of mooring lines on the dock when a vessel is made fast or let go, in the United States or the coastal waters thereof.

Subtitle H—Miscellaneous Provisions

* * * * * * *

[SEC. 879. OFFICE OF INTERNATIONAL AFFAIRS.

[(a) ESTABLISHMENT.—There is established within the Office of the Secretary an Office of International Affairs. The Office shall be headed by a Director, who shall be a senior official appointed by the Secretary.

[(b) DUTIES OF THE DIRECTOR.—The Director shall have the following duties:

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

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

[(B) Joint training exercises of first responders.

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

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

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

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

* * * * * * *

TITLE XVIII—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN

Subtitle A—General Provisions

SEC. 1801. STRATEGIC PLAN TO ENHANCE THE SECURITY OF THE INTERNATIONAL SUPPLY CHAIN.

(a) STRATEGIC PLAN.—The Secretary, in consultation with appropriate Federal, State, local, and tribal government agencies and private sector stakeholders responsible for security matters that affect or relate to the movement of containers through the international supply chain, shall develop and implement, and update as appropriate, a strategic plan to enhance the security of the international supply chain.

(b) REQUIREMENTS.—The strategic plan required under subsection (a) shall—

(1) describe the roles, responsibilities, and authorities of Federal, State, local, and tribal government agencies and private sector stakeholders that relate to the security of the movement of containers through the international supply chain;

(2) identify and address gaps and unnecessary overlaps in the roles, responsibilities, or authorities described in paragraph (1);

(3) identify and make recommendations regarding legislative, regulatory, and organizational changes necessary to improve coordination among the entities or to enhance the security of the international supply chain;

(4) provide measurable goals, including objectives, mechanisms, and a schedule, for furthering the security of commercial operations from point of origin to point of destination;

(5) build on available resources and consider costs and benefits;

(6) provide incentives for additional voluntary measures to enhance cargo security, as determined by the Secretary;

(7) consider the impact of supply chain security requirements on small and medium size companies;

(8) include a process for sharing intelligence and information with private sector stakeholders to assist in their security efforts;

(9) identify a framework for prudent and measured response in the event of a transportation security incident involving the international supply chain;

(10) provide a plan for the expeditious resumption of the flow of legitimate trade in accordance with section 70103(a)(2)(J)(ii) of title 46, United States Code;

(11) consider the linkages between supply chain security and security programs within other systems of movement, including travel security and terrorism finance programs; and

(12) expand upon and relate to existing strategies and plans, including the National Strategy for Maritime Security and the eight supporting plans of the Strategy, as required by Homeland Security Presidential Directive-13 (September 2005).

(c) UTILIZATION OF ADVISORY COMMITTEES.—As part of the consultations described in subsection (a), the Secretary shall, to the extent practicable, utilize the Homeland Security Advisory Committee,

the National Maritime Security Advisory Committee, and the Commercial Operations Advisory Committee to review, as necessary, the draft strategic plan and any subsequent updates to the strategic plan.

(d) INTERNATIONAL STANDARDS AND PRACTICES.—In furtherance of the strategic plan required under subsection (a), the Secretary is encouraged to consider proposed or established standards and practices of foreign governments and international organizations, including the International Maritime Organization, the World Customs Organization, the International Labor Organization, and the International Organization for Standardization, as appropriate, to establish standards and best practices for the security of containers moving through the international supply chain.

(e) REPORT.—

(1) INITIAL REPORT.—The Secretary shall submit to the appropriate congressional committees a report that contains the strategic plan required by subsection (a).

(2) FINAL REPORT.—Not later than three years after the date on which the strategic plan is submitted under paragraph (1), the Secretary shall submit to the appropriate congressional committees a report that contains an update of the strategic plan.

(f) DEFINITION.—In this section, the term "transportation security incident" has the meaning given the term in section 70101(6) of title 46, United States Code.

SEC. 1802. TRANSMISSION OF ADDITIONAL DATA ELEMENTS FOR IMPROVED HIGH RISK TARGETING.

(a) REQUIREMENT.—The Secretary shall require transmission to the Department, through an electronic data interchange system, of additional data elements for improved high risk targeting, including appropriate security elements of entry data, as determined by the Secretary, to be provided as advanced information with respect to cargo destined for importation into the United States prior to loading of such cargo on vessels at foreign seaports.

(b) REGULATIONS.—The Secretary shall promulgate regulations to carry out this section. In promulgating such regulations, the Secretary shall adhere to the parameters applicable to the development of regulations under section 343(a) of the Trade Act of 2002 (19 U.S.C. 2071 note), including provisions relating to consultation, technology, analysis, use of information, confidentiality, and timing requirements.

SEC. 1803. PLAN TO IMPROVE THE AUTOMATED TARGETING SYSTEM.

(a) PLAN.—The Secretary shall develop and implement a plan to improve the Automated Targeting System for the identification of high-risk containers moving through the international supply chain.

(b) CONTENTS.—

(1) TREATMENT OF RECOMMENDATIONS.—The Secretary shall include in the plan required under subsection (a) a schedule to address the recommendations of the Comptroller General of the United States, the Inspector General of the Department of the Treasury, and the Inspector General of the Department of Homeland Security with respect to the operation of the Automated Targeting System.

(2) INFORMATION SUBMISSIONS.—In developing the plan required under subsection (a), the Secretary shall consider the cost, benefit, and feasibility of—

(A) requiring additional nonmanifest documentation for each container;

(B) adjusting the time period allowed by law for revisions to a container cargo manifest;

(C) adjusting the time period allowed by law for submission of entry data for vessel or cargo; and

(D) such other actions the Secretary considers beneficial for improving the information relied upon for the Automated Targeting System and any other targeting systems in furthering the security and integrity of the international supply chain.

(3) OUTSIDE REVIEW.—The Secretary shall conduct, through an independent panel, a review of the Automated Targeting System. The results of this review shall be included in the plan required under subsection (a).

(4) SMART SYSTEM.—The Secretary shall consider future iterations of the Automated Targeting System, which would incorporate smart features, such as more complex algorithms and real-time intelligence, instead of relying solely on rule sets that are periodically updated. The Secretary shall also consider how the Automated Targeting System could be improved through linkages with targeting systems in existence on the date of the enactment of the Security and Accountability For Every Port Act for travel security and terrorism finance programs.

(c) NEW OR EXPANDED INFORMATION SUBMISSIONS.—In considering any new or expanded information submission requirements, the Secretary shall consult with stakeholders and identify the need for such information, appropriate confidentiality requirements with respect to such information, and appropriate timing of the submission of such information, in the plan required under subsection (a).

(d) SECURE TRANSMISSION OF CERTAIN INFORMATION.—All information required by the Department from supply chain partners shall be transmitted in a secure fashion, as determined by the Secretary, so as to protect the information from unauthorized access.

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated $5,000,000 for each of the fiscal years 2007 through 2012 to carry out this section.

SEC. 1804. CONTAINER STANDARDS AND VERIFICATION PROCEDURES.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Secretary shall establish minimum standards and verification procedures for securing containers in transit to the United States relating to the sealing of containers.

(2) DEADLINE FOR ENFORCEMENT.—Not later than two years after the date on which the standards and procedures are established pursuant to paragraph (1), all containers bound for ports of entry in the United States shall meet such standards and procedures.

(b) REVIEW AND ENHANCEMENT.—The Secretary shall regularly—

(1) review the standards and procedures established pursuant to subsection (a); and

(2) enhance the security standards and procedures, as appropriate, based on tests of technologies as they become commer-

cially available to detect container intrusion and the highest consequence threats, particularly weapons of mass destruction.

(c) INTERNATIONAL CARGO SECURITY STANDARDS.—The Secretary, in consultation with the Secretary of State, is encouraged to promote and establish international standards for the security of containers moving through the international supply chain with foreign governments and international organizations, including the International Maritime Organization and the World Customs Organization.

(d) INTERNATIONAL TRADE AND OTHER OBLIGATIONS.—In carrying out this section, the Secretary shall consult with appropriate Federal departments and agencies and private sector stakeholders to ensure that actions under this section do not violate international trade obligations or other international obligations of the United States.

SEC. 1805. CONTAINER SECURITY INITIATIVE (CSI).

(a) AUTHORIZATION.—The Secretary is authorized to establish and implement a program (to be known as the "Container Security Initiative" or "CSI") to identify and examine maritime containers that pose a risk for terrorism at foreign ports before the containers are shipped to the United States.

(b) ASSESSMENT.—Before the Secretary designates any foreign port under CSI, the Secretary, in consultation with other Federal officials, as appropriate, shall conduct an assessment of the port, including—

(1) the level of risk for the potential compromise of containers by terrorists or terrorist weapons;

(2) the volume of regular container traffic to United States ports;

(3) the results of the Coast Guard assessments conducted pursuant to section 70108 of title 46, United States Code;

(4) the commitment of the host nation to cooperating with the Department in sharing critical data and risk management information and to maintain programs to ensure employee integrity; and

(5) the potential for validation of security practices by the Department.

(c) NOTIFICATION.—The Secretary shall notify the appropriate congressional committees prior to notifying the public of the designation of a foreign port under CSI.

(d) INSPECTIONS.—

(1) REQUIREMENTS AND PROCEDURES.—The Secretary shall—

(A) establish technical capability criteria and standard operating procedures for the use of nonintrusive inspection and nuclear and radiological detection systems in conjunction with CSI;

(B) require each port designated under CSI to operate nonintrusive inspection and nuclear and radiological detection systems in accordance with the technical capability criteria and standard operating procedures established under subparagraph (A); and

(C) continually monitor the technologies, processes, and techniques used to inspect cargo at ports designated under CSI.

(2) CONSISTENCY OF STANDARDS AND PROCEDURES.—The Secretary shall ensure that the technical capability criteria and

standard operating procedures established under paragraph (1)(A) are consistent with such standards and procedures of any other department or agency of the Federal government with respect to deployment of nuclear and radiological detection systems outside the United States.

(3) FOREIGN ASSISTANCE.—

(A) IN GENERAL.—The Secretary, in consultation with the Secretary of State, the Secretary of Energy, and the heads of other Federal agencies, shall identify foreign assistance programs that could facilitate the implementation of cargo security antiterrorism measures at ports designated under CSI and foreign ports not designated under CSI that lack effective antiterrorism measures.

(B) ACQUISITION.—The Secretary is authorized to loan or otherwise assist in the deployment of nonintrusive inspection or nuclear and radiological detection systems for cargo containers at each designated CSI port under such terms and conditions as the Secretary determines to be appropriate and to provide training for foreign personnel involved in CSI.

(e) PROHIBITION.—

(1) IN GENERAL.—The Secretary shall issue a "do not load" order to each port designated under CSI to prevent the onload of any cargo that has been identified as higher risk by the Automated Targeting System unless the cargo—

(A) is scanned with a non intrusive imagery device and nuclear or radiological detection equipment;

(B) is devanned and inspected with nuclear or radiological detection equipment; or

(C) is determined to be of lower risk following additional inquiries by appropriate personnel of U.S. Customs and Border Protection.

(2) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to interfere with the ability of the Secretary to deny entry of any cargo into the United States.

(f) REPORT.—The Secretary shall submit to the appropriate congressional committees not later than March 1 of each year a report on the status of CSI, including—

(1) a description of the security improvements gained through CSI;

(2) the rationale for the continuance of each port designated under CSI;

(3) an assessment of the personnel needs at each port designated under CSI; and

(4) a description of the potential for remote targeting to decrease the number of personnel who are deployed at foreign ports under CSI.

(g) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated $196,000,000 for each of the fiscal years 2007 through 2012 to carry out this section.

SEC. 1806. INFORMATION SHARING RELATING TO SUPPLY CHAIN SECURITY COOPERATION.

(a) PURPOSES.—The purposes of this section are—

(1) to establish continuing liaison and to provide for supply chain security cooperation between Department and the private sector; and

(2) to provide for regular and timely interchange of information between the private sector and the Department concerning developments and security risks in the supply chain environment.

(b) SECURE SYSTEM.—The Secretary shall develop a secure electronic data interchange system to collect from and share appropriate risk information related to securing the supply chain with the private sector entities determined appropriate by the Secretary.

(c) CONSULTATION.—In developing the system under subsection (b), the Secretary shall consult with the Commercial Operations Advisory Committee and a broad range of public and private sector entities likely to utilize the system, including importers, exporters, carriers, customs brokers, and freight forwarders, among other parties.

(d) PROCEDURES.—The Secretary shall establish uniform procedures for the receipt, care, and storage of supply chain security information that is voluntarily submitted to the Department through the system developed under subsection (b).

(e) LIMITATIONS.—The voluntary information collected through the system developed under subsection (b) shall be used exclusively for ensuring security and shall not be used for determining entry or for any other commercial enforcement purpose. The voluntary information submitted to the Department through the system developed under subsection (b) shall not be construed to constitute compliance with any requirement to submit such information to a Federal agency under any other provision of law.

(f) PARTICIPANTS.—The Secretary shall develop protocols for determining appropriate private sector personnel who shall have access to the system developed under subsection (b). Such personnel shall include designated security officers within companies that are determined to be low risk through participation in the Customs-Trade Partnership Against Terrorism program established pursuant to subtitle B of this title.

(g) CONFIDENTIALITY.—Notwithstanding any other provision of law, information that is voluntarily submitted by the private sector to the Department through the system developed under subsection (b)—

(1) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act);

(2) shall not, without the written consent of the person or entity submitting such information, be used directly by the Department or a third party, in any civil action arising under Federal or State law if such information is submitted in good faith; and

(3) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this section, except—

(A) in furtherance of an investigation or other prosecution of a criminal act; or

(B) when disclosure of the information would be—

(i) to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(ii) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the Comptroller General.

(h) INDEPENDENTLY OBTAINED INFORMATION.—Nothing in this section shall be construed to limit or otherwise affect the ability of a Federal, State, or local, government entity, under applicable law, to obtain supply chain security information, including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law.

(i) PENALTIES.—Whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any supply chain security information protected in this section from disclosure, shall be fined under title 18, United States Code, imprisoned not more than 1 year, or both, and shall be removed from office or employment.

(j) AUTHORITY TO ISSUE WARNINGS.—The Secretary may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential risks to the supply chain as appropriate. In issuing a warning, the Secretary shall take appropriate actions to protect from disclosure—

(1) the source of any voluntarily submitted supply chain security information that forms the basis for the warning; and

(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

Subtitle B—Customs-Trade Partnership Against Terrorism (C-TPAT)

SEC. 1811. ESTABLISHMENT.

(a) ESTABLISHMENT.—The Secretary is authorized to establish a voluntary program (to be known as the "Customs-Trade Partnership Against Terrorism" or "C–TPAT") to strengthen and improve the overall security of the international supply chain and United States border security.

(b) MINIMUM SECURITY REQUIREMENTS.—The Secretary shall review the minimum security requirements of C–TPAT at least once every year and update such requirements as necessary.

SEC. 1812. ELIGIBLE ENTITIES.

Importers, brokers, forwarders, air, sea, land carriers, and other entities in the international supply chain and intermodal transportation system are eligible to apply to voluntarily enter into partnerships with the Department under C-TPAT.

SEC. 1813. MINIMUM REQUIREMENTS.

An applicant seeking to participate in C–TPAT shall—

(1) demonstrate a history of moving commerce in the international supply chain;

(2) conduct an assessment of its supply chains based upon security criteria established by the Secretary, including—

(A) business partner requirements;

(B) container security;

(C) physical security and access controls;

(D) personnel security;

(E) procedural security;

(F) security training and threat awareness; and

(G) information technology security;

(3) implement and maintain security measures and supply chain security practices meeting security criteria; and

(4) meet all other requirements established by the Secretary.

SEC. 1814. TIER ONE PARTICIPANTS.

(a) BENEFITS.—The Secretary may offer limited benefits to C–TPAT participants whose security measures and supply chain security practices have been certified in accordance with the guidelines established pursuant to subsection (b).

(b) GUIDELINES.—The Secretary shall update guidelines for certifying a C-TPAT participant's security measures and supply chain security practices under this section.

SEC. 1815. TIER TWO PARTICIPANTS.

(a) IN GENERAL.—Not later than one year after a C-TPAT participant has been certified under section 1814, the Secretary shall validate, directly or through third party entities certified in accordance with section 1817, the security measures and supply chain security practices of that participant. Such validation shall include assessments at appropriate foreign locations utilized by the participant as part of the supply chain.

(b) CONSEQUENCES FOR FAILED VALIDATION.—If a C–TPAT participant's security measures and supply chain security practices fail to meet the validation requirements under this section, the Commissioner of U.S. Customs and Border Protection may—

(1) deny the participant benefits under C–TPAT on a temporary or permanent basis; or

(2) suspend or expel the participant from C–TPAT.

(c) RIGHT OF APPEAL.—A C–TPAT participant described in subsection (b) may file an appeal with the Secretary of the Commissioner's decision under subsection (b)(1) to deny benefits under C–TPAT or under subsection (b)(2) to suspend or expel the participant from C–TPAT.

(d) BENEFITS.—The Secretary shall extend benefits to each C-TPAT participant that has been validated under this section, which may include—

(1) reduced examinations; and

(2) priority processing for searches.

SEC. 1816. TIER THREE PARTICIPANTS.

(a) IN GENERAL.—The Secretary shall establish a third tier of C-TPAT that offers additional benefits to C-TPAT participants that demonstrate a sustained commitment beyond the minimum criteria for participation in C-TPAT.

(b) ADDITIONAL CRITERIA.—The Secretary shall designate criteria for C-TPAT participants under this section that may include criteria to ensure—

(1) cargo is loaded on a vessel with a vessel security plan approved under section 70103(c) of title 46, United States Code, or on a vessel with a valid International Ship Security Certificate as provided for under part 104 of title 33, Code of Federal Regulations;

(2) container security devices and related policies and practices that exceed the standards and procedures established by the Secretary are utilized; and

(3) cargo complies with any other requirements determined by the Secretary.

(c) BENEFITS.—The Secretary, in consultation with the Commercial Operations Advisory Committee and the National Maritime Security Advisory Committee, may provide benefits to C-TPAT participants under this section, which may include—

(1) the expedited release of tier three cargo into destination ports within the United States during all threat levels designated by the Secretary;

(2) reduced or streamlined bonding requirements that are consistent with obligations under other applicable provisions of law;

(3) preference to vessels;

(4) further reduced examinations;

(5) priority processing for examinations;

(6) further reduced scores in the Automated Targeting System; and

(7) streamlined billing of any customs duties or fees.

(d) DEFINITION.—In this section, the term "container security device" means a mechanical or electronic device designed to, at a minimum, detect unauthorized intrusion of containers.

SEC. 1817. CONSEQUENCES FOR LACK OF COMPLIANCE.

(a) IN GENERAL.—If a C–TPAT participant's security measures and supply chain security practices fail to meet any of the requirements under this subtitle, the Secretary may deny the participant benefits in whole or in part under this subtitle.

(b) FALSE OR MISLEADING INFORMATION.—If a C-TPAT participant intentionally provides false or misleading information to the Secretary or a third party entity during the validation process of the participant under this subtitle, the Commissioner of U.S. Customs and Border Protection shall suspend or expel the participant from C-TPAT for a period of not less than five years.

(c) RIGHT OF APPEAL.—A C–TPAT participant described in subsection (a) may file an appeal with the Secretary of the Secretary's decision under subsection (a) to deny benefits under this subtitle. A C-TPAT participant described in subsection (b) may file an appeal with the Secretary of the Commissioner's decision under subsection (b) to suspend or expel the participant from C-TPAT.

SEC. 1818. VALIDATIONS BY THIRD PARTY ENTITIES.

(a) IN GENERAL.—In conducting the pilot program under subsection (f), and if the Secretary determines to expand the use of third party entities to conduct validations of C-TPAT participants

upon completion of the pilot program under subsection (f), the Secretary shall—

(1) develop, document, and update, as necessary, minimum standard operating procedures and requirements applicable to such entities for the conduct of such validations; and

(2) meet all requirements under subtitle G of the title VIII of this Act to review and designate such minimum standard operating procedures as a qualified anti-terrorism technology for purposes of such subtitle.

(b) CERTIFICATION OF THIRD PARTY ENTITIES.—

(1) ISSUANCE OF CERTIFICATE OF CONFORMANCE.—In accordance with section 863(d)(3) of this Act, the Secretary shall issue a certificate of conformance to a third party entity to conduct validations under this subtitle if the entity—

(A) demonstrates to the satisfaction of the Secretary the ability to perform validations in accordance with standard operating procedures and requirements (or updates thereto) designated as a qualified anti-terrorism technology by the Secretary under subsection (a); and

(B) agrees—

(I) to perform validations in accordance with such standard operating procedures and requirements (or updates thereto); and

(ii) to maintain liability insurance coverage at policy limits and in accordance with conditions to be established by the Secretary pursuant to section 864 of this Act; and

(C) signs an agreement to protect all proprietary information of C-TPAT participants with respect to which the entity will conduct validations.

(2) LITIGATION AND RISK MANAGEMENT PROTECTIONS.—A third party entity that maintains liability insurance coverage at policy limits and in accordance with conditions to be established by the Secretary pursuant to section 864 of this Act and receives a certificate of conformance under paragraph (1) shall receive all applicable litigation and risk management protections under sections 863 and 864 of this Act.

(3) RECIPROCAL WAIVER OF CLAIMS.—A reciprocal waiver of claims shall be deemed to have been entered into between a third party entity that receives a certificate of conformance under paragraph (1) and its contractors, subcontractors, suppliers, vendors, customers, and contractors and subcontractors of customers involved in the use or operation of the validation services of the third party entity.

(c) INFORMATION FOR ESTABLISHING LIMITS OF LIABILITY INSURANCE.—A third party entity seeking a certificate of conformance under subsection (b)(1) shall provide to the Secretary necessary information for establishing the limits of liability insurance required to be maintained by the entity under section 864(a) of this Act.

(d) ADDITIONAL REQUIREMENTS.—The Secretary shall ensure that—

(1) any third party entity under this section—

(A) has no beneficial interest in or any direct or indirect control over the C-TPAT participant that is contracting for the validation services; and

(B) has no other conflict of interest with respect to the C-TPAT participant; and

(2) the C-TPAT participant has entered into a contract with the third party entity under which the C-TPAT participant agrees to pay all costs associated with the validation.

(e) MONITORING.—

(1) IN GENERAL.—The Secretary shall regularly monitor and inspect the operations of a third party entity conducting validations under this subtitle to ensure that the entity is meeting the minimum standard operating procedures and requirements for the validation of C-TPAT participants established under subsection (a) and all other applicable requirements for validation services under this subtitle.

(2) REVOCATION.—If the Secretary finds that a third party entity is not meeting the minimum standard operating procedures and requirements, the Secretary shall—

(A) revoke the entity's certificate of conformance issued under subsection (b)(1); and

(B) review any validations conducted by the entity.

(f) PILOT PROGRAM.—

(1) IN GENERAL.—The Secretary shall carry out a pilot program to test the feasibility, costs, and benefits of utilizing third party entities to conduct validations of C-TPAT participants. In conducting the pilot program, the Secretary shall comply with all applicable requirements of this section with respect to eligibility of third party entities to conduct validations of C-TPAT participants.

(2) REPORT.—Not later than 30 days after the completion of the pilot program conducted pursuant to paragraph (1), the Secretary shall submit to the appropriate congressional committees a report that contains—

(A) the results of the pilot program; and

(B) the determination of the Secretary whether or not to expand the use of third party entities to conduct validations of C-TPAT participants.

SEC. 1819. REVALIDATION.

The Secretary shall establish a process for revalidating C-TPAT participants under this subtitle. Such revalidation shall occur not less frequently than once during every 3-year period following the initial validation.

SEC. 1820. NON-CONTAINERIZED CARGO.

The Secretary may consider the potential for participation in C-TPAT by importers of non-containerized cargoes that otherwise meet the requirements under this subtitle.

SEC. 1821. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated $75,000,000 for each of the fiscal years 2007 through 2012 to carry out this subtitle.

Subtitle C—Miscellaneous Provisions

SEC. 1831. RESEARCH, DEVELOPMENT, TEST, AND EVALUATION EFFORTS IN FURTHERANCE OF MARITIME AND CARGO SECURITY.

(a) IN GENERAL.—The Secretary shall—

(1) direct research, development, test, and evaluation efforts in furtherance of maritime and cargo security;

(2) encourage the ingenuity of the private sector in developing and testing technologies and process innovations in furtherance of these objectives; and

(3) evaluate such technologies.

(b) COORDINATION.—The Secretary, in coordination with the Undersecretary for Science and Technology, the Director of the Domestic Nuclear Detection Office of the Department, and the heads of other appropriate offices or entities of the Department, shall ensure that—

(1) research, development, test, and evaluation efforts funded by the Department in furtherance of maritime and cargo security are coordinated to avoid duplication of efforts; and

(2) the results of such efforts are shared throughout the Department and other Federal, State, and local agencies, as appropriate.

SEC. 1832. GRANTS UNDER OPERATION SAFE COMMERCE.

(a) IN GENERAL.—The Secretary shall provide grants, as part of Operation Safe Commerce, to—

(1) integrate nonintrusive imaging inspection and nuclear and radiological detection systems with automatic identification methods for containers, vessels, and vehicles;

(2) test physical access control protocols and technologies to include continuous tracking devices that provide real-time monitoring and reporting;

(3) create a data sharing network capable of transmitting data required by entities participating in the international supply chain from every intermodal transfer point to the National Targeting Center of the Department; and

(4) otherwise further maritime and cargo security, as determined by the Secretary.

(b) SUPPLY CHAIN SECURITY FOR SPECIAL CONTAINER AND NONCONTAINERIZED CARGO.—In providing grants under subsection (a), the Secretary shall establish demonstration projects that further the security of the international supply chain, including refrigerated containers, and noncontainerized cargo, including roll-on/roll-off, break-bulk, liquid, and dry bulk cargo, through real-time, continuous tracking technology for special or high-risk container cargo that poses unusual potential for human or environmental harm.

(c) COMPETITIVE SELECTION PROCESS.—The Secretary shall select recipients of grants under subsection (a) through a competitive process on the basis of the following criteria:

(1) The extent to which the applicant can demonstrate that personnel, laboratory, and organizational resources will be available to the applicant to carry out the activities authorized under this section.

(2) The applicant's capability to provide leadership in making national and regional contributions to the solution of maritime and cargo security issues.

(3) The extent to which the applicant's programs, projects, and activities under the grant will address highest risk priorities as determined by the Secretary.

(4) The extent to which the applicant has a strategic plan for carrying out the programs, projects, and activities under the grant.

(5) Any other criteria the Secretary determines to be appropriate.

(d) ADMINISTRATIVE PROVISIONS.—

(1) PROHIBITION ON DUPLICATION OF EFFORT.—Before providing any grant under subsection (a), the Secretary shall coordinate with other Federal departments and agencies to ensure the grant will not duplicate work already being carried out with Federal funding.

(2) ACCOUNTING, REPORTING, AND REVIEW PROCEDURES.—The Secretary shall establish accounting, reporting, and review procedures to ensure that—

(A) amounts made available under a grant provided under subsection (a)—

(i) are used for the purpose for which such amounts were made available; and

(ii) are properly accounted for; and

(B) amounts not used for such purpose and amounts not expended are recovered.

(3) RECORDKEEPING.—The recipient of a grant under subsection (a) shall keep all records related to expenditures and obligations of amounts provided under the grant and make such records available upon request to the Secretary for audit and examination.

(4) REVIEW.—The Secretary shall annually review the programs, projects, and activities carried out using amounts made available under grants provided under subsection (a) to ensure that obligations and expenditures of such amounts are consistent with the purposes for which such amounts are made available.

(e) ANNUAL REPORT.—Not later than March 1 of each year, the Secretary shall submit to the appropriate congressional committees a report detailing the results of Operation Safe Commerce.

(f) DEFINITION.—In this section, the term "Operation Safe Commerce" means the research, development, test, and evaluation grant program that brings together private sector shareholders, port officials, and Federal, State, and local representatives to analyze existing security procedures for cargo and develop new security protocols that have the potential to increase the security of cargo shipments by monitoring the movement and integrity of cargo through the international supply chain.

(g) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—Subject to paragraph (2), there are authorized to be appropriated $25,000,000 for each of fiscal years 2007 through 2012 to carry out this section.

(2) EFFECTIVE DATE.—Paragraph (1) shall be effective beginning on the date on which the Secretary submits to the appropriate congressional committees a report on the implementation and results of grants provided under Operation Safe Commerce before the date of the enactment of the Security and Accountability For Every Port Act.

SEC. 1833. DEFINITIONS.

In this title, the following definitions apply:

(1) AUTOMATED TARGETING SYSTEM.—The term "Automated Targeting System" means the rules-based system incorporating intelligence material and import transaction history, established by U.S. Customs and Border Protection to target high risk shipments of cargo.

(2) EXAMINATION.—The term "examination" means a physical inspection or the imaging and radiation screening of a conveyance using non-intrusive inspection (NII) technology, for the presence of contraband.

(3) INSPECTION.—The term "inspection" means the comprehensive process used by U.S. Customs and Border Protection for assessing goods entering the United States to appraise them for duty purposes, to detect the presence of restricted or prohibited items, and to ensure compliance with all applicable laws. This process may include screening, conducting an examination, or conducting a search.

(4) INTERNATIONAL SUPPLY CHAIN.—The term "international supply chain" means the end-to-end process for shipping goods from a point of origin overseas to and from the United States.

(5) NUCLEAR AND RADIOLOGICAL DETECTION SYSTEM.—The term "nuclear and radiological detection system" means any technology that is capable of detecting or identifying nuclear and radiological material or explosive devices.

(6) SCREENING.—The term "screening" means a visual or automated review of information about goods, including manifest or entry documentation accompanying a shipment being imported into the United States, to determine or assess the threat of such cargo.

(7) SEARCH.—The term "search" means an intrusive examination in which a container is opened and its contents are devanned and visually inspected for the presence of misdeclared, restricted, or prohibited items.

[TITLE VI—TREATMENT OF CHARITABLE TRUSTS FOR MEMBERS OF THE ARMED FORCES OF THE UNITED STATES AND OTHER GOVERNMENTAL ORGANIZATIONS]

TITLE XIX—MISCELLANEOUS PROVISIONS

SEC. [601.] *1901.* TREATMENT OF CHARITABLE TRUSTS FOR MEMBERS OF THE ARMED FORCES OF THE UNITED STATES AND OTHER GOVERNMENTAL ORGANIZATIONS.

(a) * * *

* * * * * * *

TITLE XX—OFFICE OF DOMESTIC NUCLEAR DETECTION

SEC. 2001. DOMESTIC NUCLEAR DETECTION OFFICE.

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

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

(c) DIRECTOR.—The Office shall be headed by a Director of Domestic Nuclear Detection, who shall be appointed by the President from among individuals nominated by the Secretary.

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

SEC. 2002. FUNCTIONS OF DIRECTOR OF THE DOMESTIC NUCLEAR DETECTION OFFICE, GENERALLY.

(a) IN GENERAL.—The Secretary shall vest in the Director the primary responsibility in the Department for—

(1) administering all nuclear and radiological detection and prevention functions and assets of the Department, including those functions vested in the Department before the enactment of the Security and Accountability For Every Port Act; and

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

(b) TRANSFER OF FUNCTIONS.—The Secretary shall transfer to the Director the authority to administer, or supervise the administration of, all functions, personnel, assets, and liabilities of all Department programs and projects relating to nuclear and radiological detection research, development, testing, and evaluation, and nuclear and radiological detection system acquisition and deployment, including with respect to functions and assets transferred by section 303(1)(B), (C), and (E) and functions, assets, and personnel transferred pursuant to section 2010(c).

SEC. 2003. GLOBAL NUCLEAR DETECTION ARCHITECTURE.

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

(b) FUNCTIONS OF DIRECTOR.—The Director shall, under subsection (a)—

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

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

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

(c) RELATIONSHIP TO OTHER DEPARTMENTS AND AGENCIES.—The authority of the Director under this section shall not affect an authority or responsibility of any other department or agency of the Federal Government with respect to the deployment of nuclear and

radiological detection systems outside the United States under any program administered by that department or agency.

SEC. 2004. RESEARCH AND DEVELOPMENT.

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

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

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

(d) COORDINATION WITH OTHER FEDERAL PROGRAMS.—The Director shall coordinate implementation of the program with other Federal agencies performing similar research and development in order to accelerate the development of effective technologies, promote technology sharing, and to avoid duplication, including through the use of the interagency coordination council established under section 2013.

SEC. 2005. SYSTEM ASSESSMENTS.

(a) IN GENERAL.—The Director shall carry out a program to test and evaluate technology for detecting nuclear explosive devices and fissile or radiological material.

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

(1) under realistic operational and environmental conditions; and

(2) against realistic adversary tactics and countermeasures.

(c) PROVISION OF TESTING SERVICES.—

(1) IN GENERAL.—The Director may, under the program, make available testing services to commercial developers of detection devices.

(2) FEES.—The Director may charge fees, as appropriate, for performance of services under this subsection.

(d) SYSTEM ASSESSMENTS.—

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

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

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

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

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

SEC. 2006. TECHNOLOGY ACQUISITION, DEPLOYMENT, SUPPORT, AND TRAINING.

(a) ACQUISITION STRATEGY.—

(1) IN GENERAL.—The Director shall develop and, subject to the availability of appropriations, execute a strategy for the acquisition and deployment of detection systems in order to implement the Department components of the global nuclear detection architecture developed under section 2003.

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

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

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

(c) OPERATIONAL SUPPORT AND PROTOCOLS.—

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

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

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

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

(e) SOLICITATION OF END-USER INPUT.—In developing requirements for the research and development program of section 2004 and requirements for the acquisition of detection systems to implement the strategy in subsection (a), the Director shall solicit input from end-users of such systems.

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

SEC. 2007. SITUATIONAL AWARENESS.

(a) DETECTION INFORMATION.—The Director—

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

(2) shall gather and archive—

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

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

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

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

(d) SECURITY.—The Director shall—

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

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

SEC. 2008. FORENSIC ANALYSIS.

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

SEC. 2009. THREAT INFORMATION.

(a) THREAT ASSESSMENTS.—The Director shall utilize classified and unclassified nuclear and radiological threat assessments in designing the global nuclear detection architecture under section 2003, prioritizing detection system deployments, and testing and optimizing system performance of that architecture, including assessments of—

(1) smuggling routes;

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

(3) relevant terrorist tradecraft and concealment methods;

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

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

(c) ANALYTICAL SUPPORT.—The Director shall request that the Secretary provide to the Director, pursuant to section 201(d)(18), the requisite intelligence and information analysis support necessary to effectively discharge the Director's responsibilities.

(d) ANALYTICAL EXPERTISE.—For the purposes of performing any of the assessments required under subsection (a), the Director, sub-

ject to the availability of appropriations, may hire professional personnel who are analysts with experience in performing nuclear and radiological threat assessments.

(e) COLLECTION REQUESTS.—The Director shall recommend to the Secretary consultation that should occur pursuant to section 201(d)(10) regarding intelligence collection to design, deploy, and support the operation of the global detection architecture under section 2003.

SEC. 2010. ADMINISTRATIVE AUTHORITIES.

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

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

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

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

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

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

SEC. 2011. REPORT REQUIREMENT.

The Director shall submit to the appropriate congressional committees an annual report on the following:

(1) The global detection strategy developed under section 2003.

(2) The status of implementation of such architecture.

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

(4) The research and development program of the Office.

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

SEC. 2012. ADVISORY COUNCIL ON NUCLEAR DETECTION.

(a) ESTABLISHMENT.—Pursuant to section 871 of this Act, the Secretary shall establish within the Office an Advisory Council on Nu-

clear Detection, which shall report to the Director (in this section referred to as the "Advisory Council").

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

(1) advise the Director on recommendations for the global nuclear detection architecture developed under section 2003(a);

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

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

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

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

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

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

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

SEC. 2013. INTERAGENCY COORDINATION COUNCIL.

The President—

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

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

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

SEC. 2014. AUTHORIZATION OF APPROPRIATIONS.

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

(1) $536,000,000 for fiscal year 2007; and

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

SEC. 2015. DEFINITIONS.

In this title:

(1) The term "Director" means the Director of the Domestic Nuclear Detection Office.

(2) The term "fissile materials" means materials capable of sustaining a nuclear chain reaction.

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

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

(5) The term "Office" means the Domestic Nuclear Detection Office.

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

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

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

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

MINORITY AND DISSENTING VIEWS

INTRODUCTION

The Committee on Homeland Security marked-up and reported H.R. 4954, the "Security and Accountability For Every Port Act," or SAFE Port Act, on Wednesday, April 26, 2006.

The Committee's bipartisan and thoughtful effort to address port security, one of the most significant homeland security challenges of our time, should be commended. The Dubai Ports World scandal finally focused the attention of the public and Congress on the issue of port security, but Democrats on this Committee and its predecessor, the Select Committee on Homeland Security, have long advocated addressing security vulnerabilities at our nation's ports. Indeed, many of the bill's provisions closely mirror H.R. 4355 introduced by Economic Security, Infrastructure Protection, and Cybersecurity (ESIP&C) Ranking Member Loretta Sanchez (D–CA) in the 108th Congress; H.R. 1731 introduced by Rep. Jane Harman (D–CA) in this Congress; and an amendment offered by Rep. Sanchez during the Committee's mark-up of H.R. 1817, the Department of Homeland Security Authorization Act for Fiscal Year 2006. Rep. Harman deserves praise for her successful effort to get H.R. 4954 introduced on a bipartisan basis, and along with other leaders involved in further shaping the bill, including Rep. Sanchez and Ranking Member Bennie G. Thompson (D–MS), we are glad to have had a role in pushing the Majority to conclude work on it. We believe that H.R. 4954 represents an important step towards improving our nation's port security.

Specifically, the bill provides $400 million in much needed assistance to port operators to help offset the costs of security regulations. It also requires the development of minimum security standards for containers so that terrorists cannot tamper with shipments in route to our ports. We are also pleased that the bill makes some enhancements to the Container Security Initiative (CSI) and Customs Trade Partnership Against Terrorism (C–TPAT) programs. These changes will close dangerous security gaps that Democrats identified years ago. Finally, we appreciate the investments this bill makes in U.S. Coast Guard command centers and to advance research and development of next-generation screening and detection systems.

H.R. 4954 was further strengthened during the mark-up by the adoption of several important Democratic amendments, including one to dramatically accelerate by ten years the completion of the Deepwater Program, the Coast Guard's effort to modernize its outdated ships and equipment. This would cut by half the anticipated timeframe for completion of the Deepwater Program.

At the same time, we are disappointed by the rejection of several key amendments that would have further strengthened supply

chain security and our nation's protections against the threat of terrorists smuggling nuclear or radiological materials into this country's ports. For example, an amendment offered by Representative Edward J. Markey (D–MA) would have required all containers entering the United States to be screened within three to five years. We will continue to advocate for the inclusion of these measures as the bill progresses through the legislative process.

TITLE I—SECURITY OF UNITED STATES SEAPORTS

The recent Dubai Ports World controversy finally brought attention to seaport security. We are pleased that Title I of the bill increases funding in the port security grant program by over $200 million a year. Democratic Members of the Committee have long called for additional funding to assist ports with the cost of complying with federal security mandates, which the Coast Guard estimates could be $5.4 billion over the next ten years. Following 9/11 a number of our major seaports conducted assessments and exercises that revealed the extent of their vulnerabilities. Additionally, a number of studies revealed the economic cost of a terrorist attack at our ports. We recognize that effective security practices must be developed with the understanding of the critical role that the flow of commerce plays in this nation's economic life. In a post–9/11 world, robust security practices are part and parcel of best business practices.

We are also pleased that this title requires the Secretary of Homeland Security to complete deployment of the Transportation Worker Identification Card (TWIC) on a specific time schedule. Congress originally required the Department of Homeland Security to begin developing TWIC in 2002, so a timeline for its implementation is long overdue. Finally, other sections in this bill will improve port security by requiring the Department to develop a long-range vessel tracking system, maritime security command centers, and protocols to resume port operations in the event of a terrorist attack.

We are pleased that a number of amendments that strengthen port security provisions in Title I were accepted. First, the bipartisan amendments offered by Reps. David Reichert (R–WA) and Bill Pascrell (D–NJ) represent a major effort to ensure that longshoreman and other personnel at ports receive the training they need to prevent and respond to terrorist attacks. Second, the amendment offered by Rep. Donna Christensen (D–USVI) to accelerate completion by more than ten years of the Deepwater Program, the Coast Guard's effort to acquire new ships and equipment, is a dramatic recognition of the need to quickly provide that agency with modern tools needed to fulfill ever-increasing demands. Third, we are pleased that three amendments that seek to enhance the flow of commerce were accepted on voice vote—(1) Rep. Christensen's amendment to create a permanent Border Patrol presence in the U.S. Virgin Islands (2) Rep. Christensen's amendment to address the unintended consequences on travelers of certain departure manifest requirements and (3) Rep. Sheila Jackson-Lee's (D–TX) amendment to require a report from the Department on the security of operations at the ten United States ports that load and unload the largest numbers of containers.

Additionally, Ranking Member Thompson successfully secured an agreement with Economic Security, Infrastructure Protection, and Cybersecurity Chairman Dan Lungren (R–CA) to address concerns about the adequacy of appeal rights for port workers in states that set stricter background requirements than those set by the Federal government. We note that the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (P.L. 109–59) already provides these appeal rights to truckers carrying hazardous materials in states that set stricter standards than those required by the Federal government. We will work to reach an agreement with the Majority on this issue before this bill reaches the floor.

On the other hand, we were disappointed by the rejection of several Democratic amendments that would have greatly strengthened port security. First, we were disappointed that an amendment offered by Ranking Member Thompson to hire 1,600 Customs and Border Protection inspectors over the next four years was rejected. We strongly believe that the hiring of these new inspectors would greatly enhance the Department's ability to ensure that far more high risk containers actually get inspected. Undoubtedly, many more inspectors will be necessary when security standards and programs are improved, and next generation screening technology is finally deployed.

We were also disappointed by the rejection of several amendments to Title I offered by Rep. Jackson-Lee. Her amendment would have allowed the use of port security grant funds to defray personnel costs during periods of elevated threat level. This would have addressed one of the largest costs ports are incurring as a result of security regulations put in place after the 9/11 attacks. Indeed, the President of the American Association of Port Authorities has asked for this flexibility in the port security grant program, writing in a letter to Chairman Peter T. King (R–NY) and Ranking Member Thompson that, "Personnel costs are a large unfunded mandate for many public ports."

Rep. Jackson-Lee's other two amendments would also have strengthened port security by focusing directly on the issue at the heart of the Dubai Ports World controversy—the security implications of foreign firms overseeing operations at American ports. One of her amendments called for a moratorium on any contracts for port operations with individuals or entities with terrorist ties. The other required the Government Accountability Office (GAO) to produce a report on the activities of foreign nationals at United States ports.

TITLE II—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN

Title II contains the core of the SAFE Port Act. It would begin to address the largest gap in our port security—the security of containers transiting the global supply chain. This bill requires the Department to create a comprehensive strategy for securing maritime container traffic—the completion of which will provide crucial direction to the Department and the international community's efforts to improve security.

We are also pleased that this title requires the submission of entry data to Customs and Border Protection (CBP) as part of the Automated Targeting System (ATS). The ATS system determines a

container's level of risk by analyzing manifest data to assess whether it should be inspected. This program is at the heart of the Department's risk-based container security policy but has been roundly criticized by both the GAO and the Department's own Inspector General (IG) for its over-reliance on manifest data for targeting. The IG found that entry data produced a more accurate risk score compared to manifest data, and recommended that the Department target containers using entry data in addition to manifests and other information. This bill requires the Department to implement the IG's recommendation.

Another vulnerability that H.R. 4954 addresses is the risk that a terrorist will tamper with a container and place a weapon of mass destruction in it at some point after its departure from a foreign port. The bill's mandate that the Department issue regulations for container seals will make it harder for a terrorist to break into a container. It will also protect normal commerce by preventing goods from being stolen.

We are also heartened that this bill authorizes and improves the C–TPAT program. ESIP&C Ranking Member Sanchez has been at the forefront of efforts to ensure that the security plans of C–TPAT participants are actually validated. Currently, only 1,545 of the 5,800 companies entitled to benefits under the program have had their security plans validated. This bill requires the Secretary to initiate a pilot project to conduct C–TPAT validations using certified-third party validators. Additionally, H.R. 4954 clarifies the steps each C–TPAT participant must take to improve security practices and the benefits that participants will be entitled to receive.

This bill also directs the Department to launch a pilot project to discover ways to inspect empty containers without disrupting commerce. Rep. Sanchez became concerned about the security risks posed by empty containers after conducting a tour of a port on the West Coast, and she requested this pilot project as a way to further examine the issue.

We are also pleased that this bill restores the Operation Safe Commerce program. Operation Safe Commerce is a pilot project that tests commercial off-the-shelf technology designed to improve container security in operational supply chains. Restoring this program allows the Department to leverage the private sector to develop technology and have it tested in a real-world environment.

Although H.R. 4954's efforts to strengthen the security of the international supply chain are considerable, we are disappointed by the Chairman's departure from Committee practice and tradition when he failed to use the pre-filed amendment roster system to consider a supply chain amendment by Rep. Ginny Brown-Waite (R–FL) that had not been shared with Democrats on the Committee prior to its introduction. While we unanimously supported Rep. Brown-Waite's amendment, the context in which it was introduced—as an obvious effort to undermine another amendment offered by Rep. Markey—was disappointing. Rep. Brown-Waite's amendment would require the Department to fully evaluate emerging screening technologies, such as technology being used in Hong Kong, and would provide some new authority to the Secretary to refuse entry to containers that come from foreign ports. While Rep. Brown-Waite's amendment is admirable, it is not a substitute for

instituting aggressive scanning of U.S.-bound containers. Our nation simply cannot continue to advance supply chain security at a snail's pace.

Rep. Markey's amendment, which was defeated largely along party lines, is a forward-looking security measure, requiring that all containers be scanned and sealed, using the best available technology, within a three to five year timeframe. The amendment also gives the Secretary authority to extend these deadlines by up to a year, if necessary. Under this reasonable and feasible approach, our nation can move closer to deploying a system to screen all containers entering the United States without hindering commerce. This position was affirmed by the Committee on Transportation and Infrastructure when it approved the same amendment, offered by Rep. Jerrold Nadler (D-NY), without controversy. Indeed, several Members of this Committee who also sit on the Committee on Transportation and Infrastructure voted against Rep. Markey's amendment, but did not oppose that same amendment when it was offered by Rep. Nadler.

The reality is that by the time a weapon of mass destruction arrives in a United States port, it is too late. We must address our security vulnerabilities long before the containers are unloaded on our soil. We have the technology to do this—the ports of Hong Kong and Boston already screen most inbound cargo, using commercially available technology without interrupting the flow of commerce. According to security expert Stephen Flynn of the Council on Foreign Relations, the cost of screening would be about $50 to $100 per container—a fraction of the standard ($4,000) cost of shipping a container from Asia to the United States, and to the average ($66,000) value of each container. Our nation must put in place this type of reasonable container screening system to protect all our ports, but Congress will have to pass Rep. Markey's amendment in order to force the Department to take this step.

We were also disappointed that Rep. Sanchez's amendment dealing with the benefits available to those companies in the first tier of the C-TPAT program was rejected. At present, companies enrolled in the C-TPAT program receive a reduced score in the ATS, thereby reducing the likelihood that their containers will be inspected. Companies receive this benefit even before the Department verifies that they are actually following their registered security plan. Although this bill creates a three-tiered system of benefits for C-TPAT participants that depends on the steps they have taken to improve security, those companies in the first tier will still receive a reduced ATS score even when their security plans have not been validated. As a result, a company with lax security measures that leave its shipments open to terrorist exploitation would still receive less scrutiny than its competitors. Rep. Sanchez's amendment prohibits companies from receiving a reduced ATS score until their security plan is validated—thereby strengthening the overall security and effectiveness of the C-TPAT program. We will continue to work to address this vulnerability.

TITLE III—DIRECTORATE FOR POLICY, PLANNING, AND INTERNATIONAL AFFAIRS

Under H.R. 4954, the Department's strategic planning and program coordination under the direction of an Under Secretary of Policy would be put in statute. We supported Secretary Michael Chertoff's decision to create this office after the completion of his Second Stage Review last year, and are pleased to authorize the creation of the Policy Directorate. We will be closely monitoring the activities of this office and will continue to call upon the Department to adopt comprehensive strategic planning and integrated policies. This portion of the bill was greatly strengthened by the acceptance of Rep. Jackson-Lee's amendment requiring that anyone appointed Under Secretary of Policy has the necessary qualifications. The President's decision to fill high-level positions at the Federal Emergency Management Agency (FEMA) with unqualified individuals, instead of seasoned professionals, contributed to the poor response to Hurricane Katrina. The responsibility for coordinating Department programs adequately and thinking about long-term strategies must be put on the shoulders of an individual who has a record of leadership in developing and implementing policy. We are also supportive of the creation of an Office of Cargo Security within the Policy Directorate to improve coordination of supply-chain security initiatives among Coast Guard, CBP, and Transportation Security Administration (TSA).

TITLE IV—OFFICE OF DOMESTIC NUCLEAR DETECTION

We are pleased that the Domestic Nuclear Detection Office (DNDO), another Second Stage Review provision that we supported, is authorized at $536 million in Title IV. The DNDO is authorized to develop a global nuclear detection architecture; implement the domestic portion of the architecture; perform transformational research and development to improve detection; and provide operational support and maintain situational awareness of the nuclear and radiological threat. In addition, we are pleased with the bill's creation of a next-generation portal monitor pilot project to place the best available detection equipment in high volume ports.

Although the DNDO provisions in the bill will improve security, the rejection of amendments offered by Prevention of Nuclear and Biological Attack Ranking Member James Langevin (D-RI) represent missed opportunities to further enhance our radiation detection capabilities. Rep. Langevin's first amendment strengthened the planning provisions in the base bill by requiring the DNDO to develop a more comprehensive, risk-based deployment strategy for radiological and nuclear detection equipment, including a timeline and analysis of costs. This amendment also would increase funds for placing radiation portal monitors at ports-of-entry by $117 million. In recent testimony before the Committee, Department officials stated that funding is one of the reasons that the deployment of radiation portal monitors is behind schedule. The threat of a terrorist detonating a dirty bomb, or worse, a nuclear weapon, requires this country to have a comprehensive detection and deter-

rent capability in place. Rep. Langevin's amendment would be a large step in that direction.

We are also disappointed that Rep. Langevin's Advanced Radiation Portal Monitor Amendment was defeated. The DNDO is in the process of awarding a contract for the Advanced Spectroscopic Portal (ASP) project. The ASP portal monitors are next-generation technology that allow security officers to determine the radiological source that causes a monitor to trigger an alarm. Knowing the cause of an alarm will permit officers to keep monitors at a high level of sensitivity without triggering false alarms and slowing commerce. While there are production issues associated with this program, the primary obstacle is the cost to deploy these systems at ports-of-entry. The Department estimates this cost at $1.3 billion. Rep. Langevin's amendment authorizes this funding, thereby enabling the Department to purchase and install these systems.

CONCLUSION

The SAFE Port Act represents a major achievement for the Committee on Homeland Security in its bipartisan efforts to secure our nation's seaports. The comprehensive nature of this legislation sets it apart from previous endeavors. We are pleased that the Majority, led by Chairman King, adopted many of the legislative ideas that Democratic Committee Members have been championing for years. The inclusion of Democratic provisions greatly enhanced the final Committee product. As this legislation weaves its way through the Congress, we will continue to seek opportunities to further strengthen H.R. 4954, the SAFE Port Act.

BENNIE G. THOMPSON.
ZOE LOFGREN.
BOB ETHERIDGE.
KENDRICK B. MEEK.
LORETTA SANCHEZ.
BILL PASCRELL, JR.
JIM LANGEVIN.
EDWARD J. MARKEY.
JANE HARMAN.
NITA LOWEY.
DONNA M. CHRISTENSEN.
NORM DICKS.
PETER DEFAZIO.
SHEILA JACKSON-LEE.
ELEANOR H. NORTON.

RALPH M. HALL, TEXAS
MICHAEL BILIRAKIS, FLORIDA
VICE CHAIRMAN
FRED UPTON, MICHIGAN
CLIFF STEARNS, FLORIDA
PAUL E. GILLMOR, OHIO
NATHAN DEAL, GEORGIA
ED WHITFIELD, KENTUCKY
CHARLIE NORWOOD, GEORGIA
BARBARA CUBIN, WYOMING
JOHN SHIMKUS, ILLINOIS
HEATHER WILSON, NEW MEXICO
JOHN B. SHADEGG, ARIZONA
CHARLES W. "CHIP" PICKERING, MISSISSIPPI
VICE CHAIRMAN
VITO FOSSELLA, NEW YORK
ROY BLUNT, MISSOURI
STEVE BUYER, INDIANA
GEORGE RADANOVICH, CALIFORNIA
CHARLES F. BASS, NEW HAMPSHIRE
JOSEPH R. PITTS, PENNSYLVANIA
MARY BONO, CALIFORNIA
GREG WALDEN, OREGON
LEE TERRY, NEBRASKA
MIKE FERGUSON, NEW JERSEY
MIKE ROGERS, MICHIGAN
C.L. "BUTCH" OTTER, IDAHO
SUE MYRICK, NORTH CAROLINA
JOHN SULLIVAN, OKLAHOMA
TIM MURPHY, PENNSYLVANIA
MICHAEL C. BURGESS, TEXAS
MARSHA BLACKBURN, TENNESSEE

BUD ALBRIGHT, STAFF DIRECTOR

ONE HUNDRED NINTH CONGRESS

U.S. House of Representatives

Committee on Energy and Commerce

Washington, DC 20515–6115

JOE BARTON, TEXAS
CHAIRMAN

JOHN D. DINGELL, MICHIGAN
RANKING MEMBER
HENRY A. WAXMAN, CALIFORNIA
EDWARD J. MARKEY, MASSACHUSETTS
RICK BOUCHER, VIRGINIA
EDOLPHUS TOWNS, NEW YORK
FRANK PALLONE, JR., NEW JERSEY
SHERROD BROWN, OHIO
BART GORDON, TENNESSEE
BOBBY L. RUSH, ILLINOIS
ANNA G. ESHOO, CALIFORNIA
BART STUPAK, MICHIGAN
ELIOT L. ENGEL, NEW YORK
ALBERT R. WYNN, MARYLAND
GENE GREEN, TEXAS
TED STRICKLAND, OHIO
DIANA DEGETTE, COLORADO
LOIS CAPPS, CALIFORNIA
MIKE DOYLE, PENNSYLVANIA
TOM ALLEN, MAINE
JIM DAVIS, FLORIDA
JAN SCHAKOWSKY, ILLINOIS
HILDA L. SOLIS, CALIFORNIA
CHARLES A. GONZALEZ, TEXAS
JAY INSLEE, WASHINGTON
TAMMY BALDWIN, WISCONSIN
MIKE ROSS, ARKANSAS

April 28, 2006

The Honorable Peter King
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman King:

I understand that you will shortly bring H.R. 4954 as reported by the Committee on Homeland Security, the SAFE Port Act, to the House floor. This legislation contains provisions that fall within the jurisdiction of the Committee on Energy and Commerce.

I recognize your desire to bring this legislation before the House in an expeditious manner. Accordingly, I will not exercise my Committee's right to a referral. By agreeing to waive its consideration of the bill, however, the Energy and Commerce Committee does not waive its jurisdiction over H.R. 4954. In addition, the Energy and Commerce Committee reserves its right to seek conferees on any provisions of the bill that are within its jurisdiction during any House-Senate conference that may be convened on this or similar legislation. I ask for your commitment to support any request by the Energy and Commerce Committee for conferees on H.R. 4954 or similar legislation.

I request that you include this letter in legislative report and the *Congressional Record* during consideration of H.R. 4954. Thank you for your attention to these matters.

Sincerely,

Joe Barton

Joe Barton
Chairman

JB/jdb

PETER T. KING, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Ninth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

April 28, 2006

The Honorable Joe Barton
Chairman
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your recent letter regarding the Energy and Commerce Committee's jurisdictional interest in H.R. 4954, the "SAFE Port" Act. The Bill was introduced on March 14, 2006, and referred solely to the Committee on Homeland Security. The Committee on Homeland Security marked up the Bill and ordered it reported on April 26, 2006.

I appreciate your willingness to waive further consideration of H.R. 4954 in order to expedite proceedings on this legislation. I agree that by not exercising your right to request a referral, the Energy and Commerce Committee does not waive any jurisdiction it may have over H.R. 4954. In addition, I agree that if any provisions of the Bill are determined to be within the jurisdiction of the Energy and Commerce Committee, I will support representation for your Committee during conference with the Senate with respect to those provisions.

As you have requested, I will include a copy of your letter and this response as part of the Committee on Homeland Security's Report and the *Congressional Record* during consideration of the legislation on the House Floor.

Thank you for your cooperation as we work towards the enactment of H.R. 4954.

Sincerely,

PETER T. KING
Chairman

cc: The Honorable J. Dennis Hastert, Speaker
The Honorable Bennie Thompson, Ranking Member
The Honorable John D. Dingell, Ranking Member
Committee on Energy & Commerce

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE
SUITE 2320 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6371
TTY: (202) 226-4410
http://www.house.gov/science/welcome.htm

April 28, 2006

The Honorable Peter T. King
Chairman
Committee on Homeland Security
H2-176 Ford House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I am writing to you concerning the jurisdictional interest of the Science Committee in matters being considered in H.R. 4954, the Security and Accountability For Every Port or SAFE Port Act. The Science Committee has particular jurisdictional interest in the sections listed below based on the Committee's black letter jurisdiction over the "National Institute of Standards and Technology (NIST) and the standardization of weights and measures." (*Rule X (o)(7)*) In addition, the Department of Homeland Security Science and Technology Directorate ("DHS S&T") facilitates and funds the development of standards for container security. The Science Committee has jurisdiction over both the S&T Directorate and other DHS research and development based on the plain language of *Rule X(o)(14)* which grants the Science Committee jurisdiction over "Scientific research, development, and demonstration, and projects therefore."

1. Title I, Subtitle B, Section 112, Port Security Training Program – Section 112 adds a new section 802 to the Homeland Security Act of 2002. The Science Committee is interested in Section 112 but has particular interest in the language dealing with National Voluntary Consensus Standards which directs the Secretary to "support the development, promulgation, and regular updating as necessary of national voluntary consensus standards for port security training" and to ensure that training provided is consistent with such standards.

2. Certain Items Contained in Title I, Subtitle C, Section 201 – Section 201 adds a new title to the Homeland Security Act of 2002. Within that title (Title XVIII), the Science Committee is interested in the following:

    a. Section 1801, Strategic Plan to Enhance the Security of the International Supply Chain – Subsection 1801(d) on International Standards and Practices encourages the Secretary, as appropriate, "to establish standards and best practices for the security of containers moving through the International Supply Chain."

b. Section 1803, Plan to Improve the Automated Targeting System – Section 1803 requires the Secretary to develop and implement "a plan to improve the Automated Targeting System for the identification of high-risk containers moving through the International Supply Chain." This section contains a number of research and development pieces with the clearest example being the language on the "Smart System," which requires the incorporation of "smart features, such as more complex algorithms" instead of relying solely on rule sets. Such an effort to move away from a system solely based on rule sets would necessitate the need for research, development, testing and evaluation of these "smart features," including the more complex algorithms mentioned. This is clearly DHS research and development and would be carried out in coordination with DHS S&T.

c. Section 1804, Container Standards and Verification Procedures – Section 1804 requires the Secretary "to review the standards and procedures established" and "enhance the security standards and procedures, as appropriate, based on tests of technologies as they become commercially available." In addition, the Secretary "is encouraged to promote and establish international standards for the security of containers."

d. Section 1831, Research, Development, Test and Evaluation Efforts in Furtherance of Maritime and Cargo Security – Section 1831 directs the Secretary to conduct maritime and cargo security research, development, test, and evaluation activities and to consider demonstration projects. It also specifies that the Secretary, acting through the Under Secretary for Science and Technology, will coordinate these efforts within the Department.

e. Section 1832, Grants Under Operation Safe Commerce – Section 1832 directs the Secretary to provide grants "to test physical access control protocols and technologies" and "establish demonstration projects."

f. Section 1833, Definitions – Section 1833 provides definitions and other administrative language relating to the prior sections.

3. Title II, Subtitle C, Section 202, Next Generation Supply Chain Security Technologies – Section 202 directs the Secretary to "evaluate the development of nuclear and radiological detection systems and other inspection technologies" and to "determine if more capable commercially available technology exists" and meets technical requirements.

4. Title II, Subtitle C, Section 206, Study and Report on Advanced Imagery Pilot Programs – Section 206 directs the Secretary to "conduct a study of the merits of current container inspection pilot programs" and to conduct "an assessment of the impact of technology." The test and evaluation of technologies required to fulfill this section are an element of technology development and a responsibility of DHS S&T.

5. Title III, Directorate for Policy, Planning, and International Affairs – This title amends the Homeland Security Act of 2002 and establishes a new directorate at the Department, the position of Under Secretary for Policy and several Assistant

Secretary positions. Several provisions in this title are of particular interest to the Science Committee, including language directing the Under Secretary for Policy "to analyze, evaluate, and review the completed, ongoing, and proposed programs of the Department." In addition, the Under Secretary for Policy is directed to promote "the exchange of information on research and development on homeland security technologies," "to plan and participate in international conferences [and] exchange programs (including the exchange of scientists, engineers and other experts)," and "to represent the Department in international negotiations, working groups, and standards-setting bodies."

6. Title IV, Office of Domestic Nuclear Detection – This title amends the Homeland Security Act of 2002 and authorizes the Office of Domestic Nuclear Detection ("DNDO") at the Department. This amendment transfers from the Under Secretary of Science and Technology to the Director of DNDO "all Department programs and projects relating to nuclear and radiological detection research, development, testing and evaluation." These activities remain within the Science Committee's jurisdiction.

The Science Committee acknowledges the importance of H.R. 4954 and the need for the legislation to move expeditiously. Therefore, while we have a claim to jurisdiction over at least the sections of the bill listed above, I agree not to request a sequential referral. This, of course, is conditional on our mutual understanding that nothing in this legislation or my decision to forgo a sequential referral waives, reduces or otherwise affects the jurisdiction of the Science Committee, and that a copy of this letter and of your response will be included in the Committee report and in the *Congressional Record* when the bill is considered on the House Floor.

The Science Committee also expects that you will support our request to be conferees on any provisions over which we have jurisdiction during any House-Senate conference on this legislation.

Thank you for your attention to this matter.

Sincerely,

SHERWOOD BOEHLERT
Chairman

cc: The Honorable John V. Sullivan

PETER T. KING, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Ninth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

April 28, 2006

The Honorable Sherwood Boehlert
Chairman
Committee on Science
2320 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your recent letter regarding the Science Committee's jurisdictional interest in H.R. 4954, the "SAFE Port" Act. The Bill was introduced on March 14, 2006, and referred solely to the Committee on Homeland Security. The Committee on Homeland Security marked up the Bill and ordered it reported on April 26, 2006.

I appreciate your willingness to waive further consideration of H.R. 4954 in order to expedite proceedings on this legislation. I agree that by not exercising your right to request a referral, the Science Committee does not waive any jurisdiction it may have over H.R. 4954. In addition, I agree that if any provisions of the Bill are determined to be within the jurisdiction of the Science Committee, I will support representation for your Committee during conference with the Senate with respect to those provisions.

As you have requested, I will include a copy of your letter and this response as part of the Committee on Homeland Security's Report and the *Congressional Record* during consideration of the legislation on the House Floor.

Thank you for your cooperation as we work towards the enactment of H.R. 4954.

Sincerely,

PETER T. KING
Chairman

cc: The Honorable J. Dennis Hastert, Speaker
The Honorable Bennie Thompson, Ranking Member
The Honorable Bart Gordon, Ranking Member
Committee on Science

http://www.house.gov/cha