109TH CONGRESS  
2D Session  

S. 2459  

To improve cargo security, and for other purposes.

IN THE SENATE OF THE UNITED STATES  

MARCH 27, 2006  

Ms. Collins (for herself, Mrs. Murray, Mr. Coleman, and Mr. Lieberman) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL  

To improve cargo security, and for other purposes.

Be it enacted by the Senate and House of Representa-
tives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.  

(a) SHORT TITLE.—This Act may be cited as the "GreenLane Maritime Cargo Security 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.  
Sec. 4. Strategy.  
Sec. 5. Under Secretary for Policy.  
Sec. 6. Container security standards and procedures.  
Sec. 7. Radiation detection and radiation safety.  
Sec. 9. Customs-Trade Partnership Against Terrorism.
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. Improving the security of this complex supply chain is critical for the prosperity and liberty of all nations.

(2) In 2004, approximately 9,700,000 shipping containers came into the United States through the Nation’s seaports, averaging nearly 27,000 per day.

(3) In May 2002, the Brookings Institution estimated that costs associated with United States port closures from a detonated terrorist weapon could add up to $1,000,000,000,000 from the resulting economic slump and changes in our Nation’s ability to trade. Although the October 2002 west coast port closures were anticipated, such closures cost the American economy approximately $1,000,000,000 per day for the first 5 days.

(4) In its final report, the National Commission on Terrorist Attacks Upon the United States noted, “While commercial aviation remains a possible tar-
get, terrorists may turn their attention to other
modes of transportation. Opportunities to do harm
are as great, or greater, in maritime or surface
transportation. Initiatives to secure shipping con-
tainers have just begun.”.

(5) The April 2005 Government Accountability
Office report entitled “CONTAINER SECURITY:
A Flexible Staffing Model and Minimum Equipment
Requirements Would Improve Overseas Targeting
and Inspection Efforts” reported that the effective-
ness of the Container Security Initiative is com-
promised when containers screened by the Bureau of
Customs and Border Protection and identified as
high-risk are not properly inspected and examined
by foreign governments.

(6) The March 2005 Government Account-
ability Office report entitled, “CARGO SECURITY:
Partnership Program Grants Importers Reduced
Scrutiny with Limited Assurance of Improved Secu-
ritv”, reports that the terrorist events of September
11, 2001, raised concerns about the potential use of
company supply chains, particularly oceangoing
cargo containers, to move weapons of mass destruc-
tion to the United States. While the likelihood of
such use of containers is considered low, the move-
ment of oceangoing containerized cargo is vulnerable
to some form of terrorist action. Such action, includ-
ing attempts to smuggle either fully assembled weap-
ons of mass destruction or their individual compo-
nents, could lead to widespread death and damage.

(7) In August 2005, the President issued the
National Strategy for Maritime Security, which
notes that the probability of a hostile state using a
weapon of mass destruction (referred to in this sec-
tion as “WMD”) will increase during the next dec-
ade. WMD are of great concern since the maritime
sector is the most likely to be used to bring a WMD
into the United States. In addition, the adoption of
a “just-in-time delivery approach to shipping by
most industries, rather than stockpiling or maintain-
ing operating reserves of energy, raw materials, and
key components, means that a disruption or slowing
of the flow of almost any item can have widespread
implications for the overall market and national
economy”.

(8) Significant enhancements can be achieved
by applying a layered approach to supply chain secu-
ritv, though such layers must be developed in a co-
ordinated fashion. Current supply chain security
programs within the Federal government have been
independently operated, often falling short of gains which could be made had coordination taken place.

(9) In a May 26, 2005, hearing of the Perma-

nent Subcommittee on Investigations of the Com-

mittee on Homeland Security and Governmental Af-

fairs of the Senate, key concerns with the Depart-

ment’s supply chain security programs were noted, including—

(A) only 17.5 percent of the cargo that the
Bureau of Customs and Border Protection had
identified as high-risk is inspected overseas;

(B) equipment, such as radiation detection
devices and nonintrusive imaging machines,
used overseas for inspections are untested and
of unknown quality;

(C) the Bureau of Customs and Border
Protection has failed to develop performance
measures for the Container Security Initiative
that would validate CSI port designations and
justify the deployment of personnel overseas;

(D) the lack of such performance measures
and an assessment for staffing allocations has
lead to some CSI ports being overstaffed while
others are inadequately staffed;
(E) substantial benefits including fewer inspections are provided to importers enrolled in the C–TPAT program without a thorough review or validation of their supply chain security profiles; and

(F) the validation procedures and requirements are not sufficiently rigorous to ensure the C–TPAT member’s security procedures are adequate.

(10) The statement of managers accompanying the conference report on the Department of Homeland Security Appropriations Act, 2005 (Public Law 108–334) directed the Under Secretary for Border and Transportation Security to “submit a report to the Congress no later than February 8, 2005, which identified: (1) the steps the Department has taken to date to enhance shipping container security, (2) the resources that have been devoted to shipping container security in prior fiscal years and the proposed resources to continue this security, (3) the results of on-going projects, such as Operation Safe Commerce, CSI, C–TPAT and others, (4) which departmental entity has primary responsibility for implementing the needed changes, and (5) the steps the entity with primary responsibility will take to
implement these changes, including a specific sched-
ule for the development and issuance of standards,
policies, procedures, or regulations.”. The statement
of managers acompañying the conference report on
the Department of Homeland Security Appropria-
tions Act, 2006 (Public Law 109–90) directed the
Department of Homeland Security to conduct a new
review regarding cargo container security, stating
“on June 9, 2005, the Department submitted a re-
port on cargo container security which was 4 months
overdue and did not meet the needs outlined in the
statement of managers accompanying the conference
report on the Department of Homeland Security Ap-
propriations Act, 2005 (Public Law 108–334).”.

(11) While it is impossible to completely remove
the risk of terrorist attacks, security measures in the
transport sector designed to counter terrorism 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, counter-
terrorism measures can also present an opportunity
to find and agree on measures that combine the im-
perative to fight terrorism with the possibility of in-
creased efficiency in the system. These efficiency gains are maximized when all nations adopt them.

(12) The World Customs Organization has taken a positive step in furtherance of international supply chain security in publishing the Framework of Standards to Secure and Facilitate Global Trade, which outlines a set of minimum standards designed to—

(A) establish standards for security and trade facilitation;

(B) enable integrated supply chain management;

(C) enhance the capabilities of customs administrations; and

(D) promote cooperation between the customs and business communities.

(13) The shipping industry has a responsibility to monitor, self-assess, and report on the risks associated with goods under their control or use. The public sector must offer incentives for companies to invest in security in order to promote information sharing and other public-benefit outcomes.

(14) Increasing the transparency of the supply chain will assist in mitigating the impact of an incident by allowing for targeted shutdown of the inter-
national supply chain and expedited restoration of commercial traffic.

SEC. 3. DEFINITIONS.

In this Act:

(1) AUTOMATED TARGETING SYSTEM.—The term “Automated Targeting System” means the system established by the Bureau of Customs and Border Protection to assess imports and target those imports which pose a high risk of containing contraband.

(2) CONTAINER.—The term “container” has the meaning given the term in the International Convention for Safe Containers, with annexes, done at Geneva December 2, 1972 (29 UST 3707).

(3) CONTAINER SECURITY DEVICE.—The term “container security device” means a device or system to track and monitor containers for, and secure them against, tampering or compromise throughout the international supply chain.

(4) CONTAINER SECURITY INITIATIVE; CSI.—The terms “Container Security Initiative” and “CSI” mean the program authorized under section 8 to identify and examine maritime containers that pose a risk for terrorism at foreign ports before they are shipped to the United States.
(5) **Customs-Trade partnership against terrorism; C–TPAT.**—The terms “Customs-Trade Partnership Against Terrorism” and “C–TPAT” mean the voluntary program authorized under section 9 to strengthen and improve the overall security of the international supply chain and United States border security.

(6) **Department.**—The term “Department” means the Department of Homeland Security.

(7) **Examination.**—The term “examination” means an inspection of cargo to detect the presence of misdeclared, restricted, or prohibited items, including an inspection using nonintrusive imaging and detection technology.

(8) **GreenLane.**—The term “GreenLane” refers to the third tier of C–TPAT, that offers additional benefits to validated C–TPAT participants that demonstrate a sustained commitment beyond the minimum requirements for participation in C–TPAT.

(9) **Inspection.**—The term “inspection” means the comprehensive process used by the Bureau of Customs and Border Protection for assessing goods entering the United States to appraise them for duty purposes, to detect the presence of re-
stricted or prohibited items, and to ensure compliance with all applicable laws. This process may include screening, conducting an examination, or conducting a search.

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

(11) OPERATION SAFE COMMERCE.—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.

(12) POINT OF ORIGIN.—The term “point of origin”, in the case of goods, means the point at which such goods are assembled into the smallest exterior packaging unit for movement through the international supply chain.

(13) SCREENING.—The term “screening” means a visual or automated review of information
about goods, including manifest or entry documenta-
tion accompanying a shipment being imported into
the United States, to determine or assess the threat
of such cargo.

(14) SEARCH.—The term “search” means an
intrusive examination in which a container is opened
and its contents are de-vanned and visually in-
spected by inspectional personnel for the presence of
misdeclared, restricted, or prohibited items.

(15) SECRETARY.—The term “Secretary”
means the Secretary of Homeland Security.

(16) SMALLEST EXTERIOR PACKAGING UNIT.—
The term “smallest exterior packaging unit” has the
meaning given such term in section 4.7a of title 19,
Code of Federal Regulations (as in effect on the
date of enactment of this Act).

(17) SUPPLY CHAIN VISIBILITY PROCEDURE.—
The term “supply chain visibility procedure” means
a system or process capable of tracking goods at the
smallest exterior packaging unit level from their
point of origin to the point of loading into a con-
tainer entering the international supply chain.

(18) TRANSPORTATION SECURITY INCIDENT.—
The term “transportation security incident” has the
meaning given such term in section 70101(6) of title 46, United States Code.

SEC. 4. STRATEGY.

(a) Strategic Plan.—

(1) In General.—Not later than 180 days after the date of enactment of this Act, 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 submit a comprehensive strategic plan to enhance international supply chain security for all modes of transportation by which containers arrive in, depart from, or move through seaports of the United States to—

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

(B) the Committee on Appropriations of the Senate;

(C) the Committee on Homeland Security of the House of Representatives; and

(D) the Committee on Appropriations of the House of Representatives.
(2) CONTENT.—The strategic plan submitted under paragraph (1) shall—

(A) clarify and delineate 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;

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

(C) build on available resources and consider costs and benefits;

(D) identify mandatory, baseline security goals, and the minimum container security standards and procedures described in section 6;

(E) provide incentives for additional voluntary measures to enhance cargo security, as determined by the Secretary and under the GreenLane Program under section 10;

(F) include a process for sharing intelligence and information with private sector stakeholders to assist in their security efforts;
(G) identify a framework for prudent and measured response in the event of a transportation security incident involving the international supply chain;

(H) provide a plan for the expeditious resumption of the flow of legitimate trade in accordance with paragraph (3);

(I) focus on the secure movement of containerized cargo through the international supply chain; and

(J) expand upon and relate to existing strategies and plans, including the National Strategy for Maritime Security.

(3) Resumption of Trade.—

(A) In General.—The Secretary shall develop 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 ensure trade lanes are restored as quickly as possible.

(B) Preferences.—In reestablishing the flow of cargo through ports of entry in the United States after a transportation security in-
incident, the Secretary shall give preference to vessels—

(i) having a vessel security plan approved or accepted under section 70103(c) of title 46, United States Code;

(ii) entering a port of entry directly from a foreign port designated under CSI or from another foreign port, as determined by the Secretary;

(iii) operated by validated C–TPAT participants; and

(iv) carrying GreenLane designated cargo.

(4) UPDATE.—Not less than 3 years after the strategic plan is submitted under paragraph (1), the Secretary shall submit an update of the strategic plan to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Homeland Security of the House of Representatives, the Committee on Appropriations of the Senate, and the Committee on Appropriations of the House of Representatives.

(5) CONSULTATIONS.—Consultations described in paragraph (1) shall focus on—
(A) designing measurable goals, including objectives, mechanisms, and a schedule, for furthering the security of the international supply chain;

(B) identifying and addressing gaps in capabilities, responsibilities, or authorities;

(C) identifying and streamlining unnecessary overlaps in capabilities, responsibilities, or authorities; and

(D) identifying and making recommendations regarding legislative, regulatory, and organizational changes necessary to improve coordination among the entities or to enhance the security of the international supply chain.

(6) UTILIZATION OF ADVISORY COMMITTEES.—As part of the consultative process, the Secretary is encouraged to 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 update to that plan.

(7) INTERNATIONAL STANDARDS AND PRACTICES.—In furtherance of the strategic plan, the Secretary is encouraged to consider proposed or es-
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.

(b) IMPROVEMENTS TO AUTOMATED TARGETING SYSTEM.—

(1) PLAN.—Not later than 90 days after the date of enactment of this Act, the Secretary shall develop and implement a plan for improving the Automated Targeting System for identifying high-risk containers moving through the international supply chain.

(2) CONTENTS.—

(A) TREATMENT OF RECOMMENDATIONS.—The Secretary shall include in the plan required under paragraph (1) a schedule for completing all outstanding corrective actions recommended by the Comptroller General of the United States, the Inspector General of the Department of the Treasury, and the Inspector
General of the Department with respect to the operation of the Automated Targeting System.

(B) INFORMATION SUBMISSIONS.—In developing the plan under paragraph (1), the Secretary shall consider the cost, benefit, and feasibility of—

(i) requiring additional nonmanifest documentation for each container, including purchase orders, shipper’s letters of instruction, commercial invoices, letters of credit, certificates of origin, advance shipping notices, vessel stow plans, and certain container status messages, when created;

(ii) reducing the time period allowed by law for revisions to a container cargo manifest;

(iii) reducing the time period allowed by law for submission of entry data for vessel or cargo; and

(iv) 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.
(C) 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 submitted under paragraph (1).

(D) 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.

(3) 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, and the appropriate timing of its submission, in the plan submitted under paragraph (1).

(4) 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.
(c) UNIFORM DATA FOR GOVERNMENT-WIDE USAGE.—

(1) ESTABLISHMENT.—The Secretary, in conjunction with representatives from the Department, the Department of Transportation, the Department of Health and Human Services, the Department of Agriculture, the Department of Commerce, the Department of State, the Department of Defense, the Department of Justice, the Department of the Interior, and other appropriate Federal agencies, as determined by the Secretary, 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 (referred to in this subsection as the “International Trade Data System”).

(2) INTERAGENCY STEERING GROUP.—The Deputy Director for Management of the Office of Management and Budget (referred to in this subsection as the “Deputy Director”), pursuant to responsibilities under chapter 36 of title 44, United States Code, shall establish an executive level, interdepartmental steering group (referred to in this sub-
section as the “Interdepartmental Steering Group”), comprised of representatives of the departments listed in paragraph (1), to coordinate, the establishment, investment in, and implementation of the International Trade Data System.

(3) IMPLEMENTATION.—Not later than 1 year after the date of enactment of this Act, the Deputy Director, through the Interdepartmental Steering Group, shall complete the development of the harmonized data set of import and export information submitted to agencies with a presence at the international border of the United States.

(4) PRIVATE SECTOR CONSULTATION.—The Secretary and the Interdepartmental Steering Group shall consult with private sector stakeholders in developing the uniform data submission requirements, procedures, and schedules.

(5) JOINT INSPECTIONS PROCEDURES.—The Deputy Director, through the Interdepartmental Steering Group, shall develop plans for longer term uses of the International Trade Data System, including facilitating joint cargo inspections by multiple Federal agencies to meet their respective requirements.
SEC. 5. UNDER SECRETARY FOR POLICY.

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

(1) by redesignating title VI and section 601 as title XVIII and section 1801, respectively, and transferring that title to the end of the Act; and

(2) by inserting after title V the following:

“TITLE VI—UNDER SECRETARY FOR POLICY

SEC. 601. UNDER SECRETARY FOR POLICY.

“(a) IN GENERAL.—There shall be in the Department an Under Secretary for Policy, who shall be appointed by the President, by and with the advice and consent of the Senate.

“(b) RESPONSIBILITIES.—Subject to the direction, authority, and control of the Secretary, the responsibilities of the Under Secretary for Policy shall be as follows:

“(1) POLICY.—

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

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

“(C) To establish and direct a formal policymaking process for the Department.
“(D) To analyze, evaluate, and review completed, ongoing, and proposed programs, to ensure they are compatible with the Secretary’s priorities, strategic plans, and policies.

“(2) STRATEGIC PLANNING.—

“(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.

“(D) To conduct reviews of the Department to ensure the implementation of this paragraph.

“(3) INTERNATIONAL RESPONSIBILITIES.—

“(A) To promote informational and educational exchange with nations friendly to the United States in order to promote sharing of best practices and technologies relating to homeland security, including—

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

“(ii) joint training exercises of first responders; and
“(iii) exchanging expertise and information on terrorism prevention, response, and crisis management.

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

“(C) To plan and undertake international conferences, exchange programs (including the exchange of scientists, engineers, and other experts), and other training activities.

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

“(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 American homeland.

“(B) To advise the Secretary on the impact of the policies, regulations, processes, and actions of the Department on the private sector.
“(C) To interface with other relevant Federal agencies with homeland security missions to assess the impact of the actions of such agencies on the private sector.

“(D) 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.

“(E) To work with Federal laboratories, federally funded research and development centers, other federally funded organizations, academia, and the private sector to develop innovative approaches to address homeland security challenges to produce and deploy the best available technologies for homeland security missions.
“(F) To promote existing public-private partnerships and develop new public-private partnerships to provide for collaboration and mutual support to address homeland security challenges.

“(G) To assist in the development and promotion of private sector best practices to secure critical infrastructure.

“(H) To coordinate industry efforts, with respect to functions of the Department, to identify private sector resources and capabilities that could be effective in supplementing Federal, State, and local government agency efforts to prevent or respond to a terrorist attack.

“(I) To coordinate among Department operating entities and with the Assistant Secretary for Trade Development of the Department of Commerce on issues related to the travel and tourism industries.”.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—


(1) in section 103—
(A) by redesignating paragraphs (6) through (10) as paragraphs (7) through (11), respectively; and 

(B) by inserting after paragraph (5) the following:

“(6) An Under Secretary for Policy.”;

(2) by striking section 879; and

(3) in the table of contents—

(A) by redesignating the items relating to title VI and section 601 as items relating to title XVIII and section 1801, respectively, and transferring the items relating to that title and section to the end of the table of contents;

(B) by striking the item relating to section 879; and

(C) by inserting before the item relating to title VII the following:

“TITLE VI—UNDER SECRETARY FOR POLICY

“Sec. 601. Under Secretary for Policy.”.

(e) Office of Cargo Security Policy.—Subtitle C of title IV of the Homeland Security Act of 2002 (6 U.S.C. 231 et seq.) is amended by adding at the end the following:
“SEC. 431. OFFICE OF CARGO SECURITY POLICY.

“(a) ESTABLISHMENT.—There is established within the Department an Office of Cargo Security Policy (referred to in this section as the ‘Office’).

“(b) PURPOSE.—The Office shall—

“(1) coordinate all Department policies and programs relating to cargo security; and

“(2) consult with stakeholders and work with other Federal agencies to establish standards and regulations and to promote best practices.

“(c) DIRECTOR.—

“(1) APPOINTMENT.—The Office shall be headed by a Director, who shall—

“(A) be appointed by the Secretary; and

“(B) report to the Under Secretary for Policy.

“(2) RESPONSIBILITIES.—The Director shall—

“(A) advise the Secretary and the Under Secretary for Policy regarding all aspects of Department programs relating to cargo security;

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

“(C) coordinate the cargo security policies and programs of the Department with other executive agencies; and
“(D) coordinate all programs of the Department relating to cargo security.”.

(d) Designation of Liaison Office of Department of State.—The Secretary of State shall designate a liaison office within the Department of State to assist the Secretary, as appropriate in negotiating cargo security related international agreements; in conducting activities under this Act; and other responsibilities as assigned by the Secretary of State.

SEC. 6. CONTAINER SECURITY STANDARDS AND PROCEDURES.

(a) Establishment.—

(1) In general.—Not later than 180 days after the date of enactment of this Act, the Secretary shall establish, by regulation, minimum standards and procedures for securing containers in transit to an importer in the United States.

(2) Information sources.—The Secretary shall use information from C–TPAT, Operation Safe Commerce, any container security program of the Directorate of Science and Technology, and other security initiatives to establish the standards and procedures described in paragraph (1). Such standards may address operation, technology use, and performance.
(3) **DEADLINE FOR ENFORCEMENT.**—Not later than 2 years after the establishment of standards and procedures under subsection (a), 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, in accordance with section 11.

(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.
SEC. 7. RADIATION DETECTION AND RADIATION SAFETY.

(a) EXAMINING CONTAINERS.—Not later than 1 year after the date of enactment of this Act, all containers entering the United States shall be examined for radiation.

(b) STRATEGY.—

(1) IN GENERAL.—Not later than 90 days after the date of enactment of this Act, the Secretary shall submit a strategy for the deployment of radiation detection equipment at all ports of entry to—

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

(B) the Committee on Appropriations of the Senate;

(C) the Committee on Homeland Security of the House of Representatives; and

(D) the Committee on Appropriations of the House of Representatives.

(2) CONTENTS.—The strategy submitted under paragraph (1) shall include—

(A) the type of equipment to be used;

(B) standard operating procedures for examining containers with such equipment;

(C) a plan detailing the environmental health and safety impacts of nonintrusive inspection technology;
(D) the Department policy for the using nonintrusive inspection equipment; and

(E) a classified annex that details plans for covert testing.

(c) RADIATION SAFETY.—Not later than 90 days after the date of enactment of this Act, the Secretary shall submit a plan, to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Appropriations of the Senate, the Committee on Homeland Security of the House of Representatives, and the Committee on Appropriations of the House of Representatives, that—

(1) details the health and safety impacts of nonintrusive inspection technology; and

(2) describes the policy of the Bureau of Customs and Border Protection for using nonintrusive inspection equipment.

SEC. 8. CONTAINER SECURITY INITIATIVE.

(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 coordination with the Secretary of State and other Federal officials, as appropriate, shall conduct an assessment of the port to evaluate costs, benefits, and other factors associated with designation, including—

1. the level of risk for the potential compromise of containers by terrorists or terrorist weapons;
2. the economic impact of cargo traveling from the foreign port in terms of trade value and volume;
3. the results of the Coast Guard assessments conducted pursuant to section 70108 of title 46, United States Code;
4. the capabilities and level of cooperation expected of the intended host country;
5. the potential for validation of security practices by the Department, directly or through certified third parties within the country in which the foreign port is located;
6. the potential for amending trade agreements to reflect participation in CSI; and
7. the potential for C–TPAT and GreenLane cargo traveling from the foreign port.
(c) **ANNUAL REPORT.**—Not later than March 1 of each year in which the Secretary proposes to designate a foreign port under CSI, the Secretary shall submit a report, in classified or unclassified form, detailing the assessment of each foreign port the Secretary is considering designating under CSI, to—

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

(2) the Committee on Appropriations of the Senate;

(3) the Committee on Homeland Security of the House of Representatives; and

(4) the Committee on Appropriations of the House of Representatives.

(d) **CURRENT CSI PORTS.**—The report under subsection (c) shall include an annual assessment justifying the continuance of each port designated under CSI as of the date of enactment of this Act.

(e) **DESIGNATION OF NEW PORTS.**—The Secretary shall not designate a foreign port under CSI unless the Secretary has completed the assessment required in subsection (b) for that port and submitted a report under subsection (e) that includes that port.

(f) **NEGOTIATIONS.**—The Secretary of State, in conjunction with the United States Trade Representative,
shall enter into trade negotiations with the government of each foreign country with a port designated under CSI, as appropriate, to ensure full compliance with the requirements under CSI.

(g) Inspections.—

(1) Requirements and procedures.—The Secretary shall—

(A) establish technical capability requirements and standard operating procedures for the use of nonintrusive inspection and radiation detection equipment in conjunction with CSI;

(B) require each port designated under CSI to operate the equipment in accordance with the requirements and procedures established under subparagraph (A); and

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

(2) Foreign assistance.—

(A) In general.—The Secretary, in coordination with the Secretary of State, the Secretary of Energy, and other Federal agencies, shall identify foreign assistance programs that could facilitate the implementation of cargo security antiterrorism measures at ports des-
ignated under CSI and foreign ports not design
ignated under CSI that lack effective antiterrorism measures.

(B) ACQUISITION.—The Secretary may lease or loan nonintrusive inspection and radiation detection equipment for containers to the government of a foreign country for use in ports participating in CSI.

(C) TRAINING.—The Secretary may provide training on the use of equipment to foreign personnel at each port designated under CSI.

(h) PERSONNEL.—The Secretary shall—

(1) annually assess the personnel needs at each port designated under CSI;

(2) deploy personnel in accordance with the assessment under paragraph (1); and

(3) consider the potential for remote targeting in decreasing the number of personnel.

SEC. 9. CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM.

(a) IN GENERAL.—

(1) AUTHORIZATION.—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

•S 2459 IS
the overall security of the international supply chain
and United States border security.

(2) CORRECTION OF DEFICIENCIES.—The Sec-
retary shall correct the deficiencies of the C–TPAT
program that were identified in the Government Ac-
countability Office report entitled “CARGO SECU-
RITY: Partnership Program Grants Importers Re-
duced Scrutiny with Limited Assurance of Improved
Security” (GAO–05–404).

(3) MINIMUM REQUIREMENTS.—The Secretary
shall promulgate regulations that describe the min-
imum requirements, program tiers, and program
benefits of C–TPAT.

(b) PARTICIPATION.—Importers, brokers, 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 De-
partment.

(c) MINIMUM REQUIREMENTS.—An applicant seek-
ing 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 Sec-
retary, 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.

(d) Certification.—

(1) Guidelines.—Not later than 180 days
after the date of enactment of this Act, the Sec-
retary shall update guidelines for certifying a par-
ticipant’s security measures and supply chain secur-
ity practices.

(2) Tier One Benefits.—The Secretary may
offer limited benefits to C–TPAT participants whose
security measures and supply chain security prac-
tices have been certified in accordance with the
guidelines established pursuant to paragraph (1).
Such benefits may not include reduced scores in the Automated Targeting System.

(c) Validation.—

(1) In General.—Not later than 1 year after a participant has been certified under subsection (d)(1), the Secretary shall validate, directly or through certified third parties, the security measures and supply chain security practices of that participant. Such validation shall include a visit to foreign locations utilized by the C–TPAT participant as part of the supply chain.

(2) Guidelines.—Not later than 180 days after the date of enactment of this Act, the Secretary shall update guidelines for validating a participant’s security measures and supply chain security practices.

(3) Consequences for Failed Validation.—If a C–TPAT participant’s security measures and supply chain security practices fail to meet validation requirements—

(A) the participant may not receive the benefits of validation; and

(B) the Commissioner of the Bureau of Customs and Border Protection may deny the participant all benefits under C–TPAT.
(4) Right of Appeal.—A C–TPAT participant described under paragraph (3) may—

(A) file an appeal with the Secretary of the Commissioner’s decision under paragraph (3)(B) to deny benefits under C–TPAT; and

(B) request revalidation.

(5) Tier Two Benefits.—The Secretary shall extend benefits to each participant who has been validated under this subsection, which may include—

(A) reduced searches;

(B) priority processing for searches; and

(C) reduced scores in the Automated Targeting System.

(f) Revalidation.—The Secretary shall establish a process for revalidating C–TPAT participants. Such revalidation shall occur not less frequently than once during every 3-year period following validation.

SEC. 10. GREENLANE DESIGNATION.

(a) Establishment.—The Secretary shall establish a third tier of C–TPAT (referred to in this section as the “GreenLane”) that offers additional benefits to validated C–TPAT participants that demonstrate a sustained commitment beyond the minimum requirements for participation in C–TPAT.
(b) Basic Requirements.—Designated GreenLane participants shall ensure that—

(1) entry data is submitted on shipments before loading;

(2) cargo is loaded at a port designated under CSI, or other foreign port as determined by the Secretary, for transit to the United States;

(3) cargo is loaded on a vessel with a vessel security plan approved or accepted under section 70103(c) of title 46, United States Code;

(4) cargo is made available for screening and examination before loading using technologies, processes or techniques, as determined by the Secretary;

(5) the supply chain visibility procedures established by the Secretary are utilized;

(6) container security devices meeting the standards and procedures established by the Secretary are utilized;

(7) cargo complies with additional security criteria established by the Secretary beyond the minimum requirements for C–TPAT participation under section 9(c), particularly in the area of access controls; and

(8) cargo complies with any other requirements determined by the Secretary.
(c) **Containers Transshipped Through Canada or Mexico Under GreenLane.**—Containers entering the United States under GreenLane at a land border port of entry shall undergo the equivalent, appropriate level of inspection and screening for potential compromise by terrorists or terrorist weapons as containers arriving at a United States port of entry from a foreign port.

(d) **Consequences for Lack of Compliance.**—

(1) **In General.**—Any participant whose security measures and supply chain security practices have been found by the Secretary to be out of compliance with any requirements of the GreenLane program shall be denied all benefits under GreenLane.

(2) **Right of Appeal.**—GreenLane participants under paragraph (1) shall have the right to appeal denial of benefits decisions to the Secretary and request redesignation under GreenLane.

(e) **Non-Containerized Cargo.**—The Secretary may consider the potential for participation in the GreenLane Program by importers of non-containerized cargoes that otherwise meet the requirements under this section.

(f) **Overseas Screening and Examinations.**—Not later than 180 days after the date of enactment of
this Act, the Secretary shall submit a strategy for screen-
ing and examining GreenLane containers overseas before
they are loaded on to vessels destined for the United
States to—

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

(2) the Committee on Appropriations of the
Senate;

(3) the Committee on Homeland Security of the
House of Representatives; and

(4) the Committee on Appropriations of the
House of Representatives.

(g) RULEMAKING.—

(1) IN GENERAL.—Not later than 1 year after
the date of enactment of this Act, the Secretary, in
consultation with private sector stakeholders, shall
promulgate regulations that establish—

(A) requirements for supply chain visibility
procedures;

(B) performance standards for container
security devices and protocols for their use;

(C) procedures for overseas screening and
examination of GreenLane containers; and

(D) any other GreenLane Program re-
quirements that the Secretary considers appro-
priate, including requirements building upon sec-

urity measures and supply chain security best

practices contained in the C–TPAT minimum

requirements set forth in section 9(e).

(2) BENEFITS.—Not later than 2 years after

the date of enactment of this Act, the Secretary, in

consultation with the Commercial Operations Advi-

sory Committee, shall promulgate regulations pro-

viding benefits for participation in the GreenLane

Program, which may include—

(A) the expedited release of GreenLane
cargo into destination ports within the United
States during all threat levels designated by the
Secretary or the Commandant of the Coast
Guard;

(B) reduced or eliminated bonding require-
ments for GreenLane cargo;

(C) preference to vessels (as described in
section 4(e)(B));

(D) further reduced searches;

(E) priority processing for searches;

(F) further reduced scores in the Auto-
mated Targeting System; and

(G) streamlined billing of any customs du-
ties or fees.
SEC. 11. JOINT OPERATIONS CENTER.

(a) Establishment.—Not later than 3 years after the date of enactment of this Act, the Secretary shall establish joint operation centers for maritime and cargo security 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) Organization.—At a minimum, a joint operations center shall be colocated with the command center for each Coast Guard sector. If a particular port is covered by a command center that is not located at that port, the Secretary shall consider virtual connectivity to maintain awareness of activities of that port and to provide other agency participation in accordance with subsection (c).

(c) Participation.—The following entities shall participate in each joint operations center for maritime and cargo security:

(1) The United States Coast Guard.

(2) The Bureau of Customs and Border Protection.

(3) The Bureau of Immigration and Customs Enforcement.

(4) The Department of Defense, as appropriate.

(6) Other Federal agencies with a presence at a particular port, as appropriate, or as otherwise selected by the Secretary.

(7) State, local, and international law enforcement and first responder agencies responsible for the port, as appropriate, or as otherwise selected by the Secretary.

(8) Port authority representatives, maritime exchanges, private sector stakeholders, and other entities subject to an Area Maritime Security Plan, as selected by the Secretary.

(d) RESPONSIBILITIES.—Each joint operations center for maritime and cargo security shall—

(1) assist, as appropriate, in the implementation of maritime transportation security plans developed under section 70103 of title 46, United States Code;

(2) implement the transportation security incident response plans required under section 70104 of such title;

(3) carry out information sharing activities consistent with those required under section 1016 of the National Security Intelligence Reform Act of 2004

(4) conduct short- and long-range vessel tracking under sections 70114 and 70115 of such title 46, United States Code; and

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

(e) Security Clearances.—The Secretary shall sponsor and expedite individuals participating in the joint operations centers 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 each joint operations center for maritime security shall act as the incident commander, unless otherwise directed under the National Response Plan.

(g) Implementation.—

(1) In General.—Not later than 180 days after the date of enactment of this Act, the Secretary shall submit an implementation plan for this section to—
(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

(B) the Committee on Appropriations of the Senate;

(C) the Committee on Homeland Security of the House of Representatives; and

(D) the Committee on Appropriations of the House of Representatives.

(2) CONTENTS.—The report submitted under paragraph (1) shall describe, for each joint operations center—

(A) the location;

(B) the specific participating entities;

(C) the implementation costs; and

(D) the necessary resources for operation and maintenance, including the cost-sharing requirements for other agencies and participants.

**SEC. 12. RESEARCH, DEVELOPMENT, TEST, AND EVALUATION.**

(a) REAUTHORIZATION OF HOMELAND SECURITY SCIENCE AND TECHNOLOGY ADVISORY COMMITTEE.—

(1) IN GENERAL.—Section 311(j) of the Homeland Security Act of 2002 (6 U.S.C. 191(j)) is amended by striking “3 years after the effective date of this Act” and inserting “on December 31, 2008”.
(2) Effective date and application.—The amendment made by paragraph (1) shall be effective as if enacted on the date of enactment of the Homeland Security Act of 2002.

(3) Advisory Committee.—The Under Secretary for Science and Technology shall utilize the Homeland Security Science and Technology Advisory Committee, as appropriate, to provide outside expertise in advancing cargo security technology.

(b) Duties of Secretary.—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.

(c) Coordination.—The Secretary, acting through the Under Secretary for Science and Technology, in consultation with the Under Secretary for Policy, the Director of Cargo Security Policy, and the Chief Financial Officer, 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, as appropriate.

(d) OPERATION SAFE COMMERCE.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary shall initiate grant projects, as part of Operation Safe Commerce, that—

(A) integrate nonintrusive inspection and radiation detection equipment with automatic identification methods for containers, vessels, and vehicles;

(B) test physical access control protocols and technologies;

(C) 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

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

(2) SUPPLY CHAIN SECURITY FOR SPECIAL CONTAINER AND NONCONTAINERIZED CARGO.—The Secretary shall consider demonstration projects that
further the security of the international supply chain
for special container cargo, including refrigerated
containers, and noncontainerized cargo, including
roll-on/roll-off, break-bulk, liquid, and dry bulk
cargo.

(3) ANNUAL REPORT.—Not later than March 1
of each year, the Secretary shall submit a report de-
tailing the results of Operation Safe Commerce to—

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

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

(C) the Committee on Appropriations of
the Senate; and

(D) the Committee on Appropriations of
the House of Representatives.

(e) GREENLANE TECHNOLOGY.—The Secretary
shall, not less frequently than once every 2 years—

(1) review the technology requirements and
standards established under section 10; and

(2) test future supply chain visibility proce-
dures, container security devices, and other systems
as they become commercially available to track and
secure containers and the smallest exterior pack-
aging units loaded into containers.
SEC. 13. PORT SECURITY GRANT PROGRAM.

(a) GRANTS AUTHORIZED.—The Secretary, acting through the Office for Domestic Preparedness, shall establish a grant program to fairly and equitably allocate Federal financial assistance—

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

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

(3) to non-Federal projects contributing to the overall security of an individual port or the system of ports in the United States, as determined by the Secretary.

(b) GRANTEE SELECTION.—In awarding grants under this Act, the Secretary shall—

(1) take into account national economic and strategic defense considerations of individual ports;

(2) strongly encourage efforts to promote—

(A) integration of port-wide security, including supply chain initiatives;

(B) information and intelligence sharing; and

(C) joint efforts, such as joint operations centers, among all port stakeholders; and
(3) consider funding major projects in phases over multiple years.

(c) MULTIPLE PHASE PROJECTS.—

(1) 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.

(2) PRIORITY.—In determining grant recipients under this section, the Secretary may give preference to continuing to fund multiyear projects that have previously received funding under this section.

(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 correct port security vulnerabilities identified through vulnerability assessments approved by the Secretary;

(3) 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 Security Plan for a port area if—
(A) the Secretary increases the threat level under the Homeland Security Advisory System to Code Orange or Code Red;

(B) the Commandant of the Coast Guard raises the Maritime Security level to MARSEC Level 2 or 3; or

(C) the Secretary otherwise authorizes such costs;

(4) 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 Security Plan if the need is based upon vulnerability assessments approved by the Secretary or identified in the Area Maritime Security Plan;

(5) to develop joint operations centers, as described under section 10, that bring together Federal, State, and local officials and stakeholders into a common operation center that is focused on area maritime and cargo security;

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

(7) to conduct port-wide exercises to strengthen emergency preparedness of Federal, State, 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) construct buildings or other physical facili-
ties, except those otherwise authorized under section
611 of the Robert T. Stafford Disaster Relief and
Emergency Assistance Act (42 U.S.C. 5121 et seq.),
including those facilities in support of subsection
(d)(5), and specifically approved by the Secretary; or

(2) acquire land, unless such use is specifically
approved by the Secretary in support of subsection
(d)(5).

(f) MATCHING REQUIREMENTS.—Except as provided
in paragraph (2), Federal funds for any eligible project
under this section shall be determined by the Secretary.

(g) APPLICATION.—

(1) IN GENERAL.—Any entity subject to an
Area Maritime Transportation Security Plan may
submit an application for a grant under this section,
at such time, in such form, and containing such in-
formation and assurances as the Secretary, working
through the Office for Domestic Preparedness, may
require.
(2) Minimum standards for payment or reimbursement.—Each application submitted under paragraph (1) shall include—

(A) a comprehensive description of—

(i) the need for the project;

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

(iii) any existing cooperation agreements with other port facilities, vessels, or organizations that benefit security of the entire port; and

(iv) the applicability of the project to the Area Maritime Transportation Security Plan; and

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

(i) addresses or corrects port security vulnerabilities identified by the Coast Guard, or through port security vulnerability assessments approved by the Secretary; and
(ii) helps to ensure compliance with
the Area Maritime Transportation Security
Plan.

(3) PROCEDURAL SAFEGUARDS.—The Sec-
retary, in consultation with the Office of the Inspec-
tor General, shall issue guidelines to establish appro-
priate 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 re-
turned.

(4) PROJECT APPROVAL REQUIRED.—The Sec-
retary may not award a grant under this section un-
less the Secretary determines that—

(A) the project to be carried out with such
grant funding—

(i) is consistent with vulnerability as-
se ssments approved by the Secretary;

(ii) supports cooperation or integra-
tion of Federal, State, local, and industry
stakeholders in the port area; and
(iii) helps to implement the Area Maritime Transportation Security Plan;

(B) sufficient funding is available to meet the matching requirement described under subsection (d);

(C) the project will be completed without unreasonable delay; and

(D) the recipient has authority to carry out the proposed project.

(h) 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 port and port facilities with respect to projects funded under this section.

(i) AUDITS AND EXAMINATIONS.—All grantees under this section shall 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.
(j) **ANNUAL REPORTS.**—Not later than 1 year after
the date of enactment of this Act, and annually thereafter
until October 1, 2013, the Secretary shall submit an un-
classified report describing regarding the progress made
in meeting the objectives of the port security grant pro-
gram established under this section to—

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

(2) the Committee on Homeland Security of the
House of Representatives;

(3) the Committee on Appropriations of the
Senate; and

(4) the Committee on Appropriations of the
House of Representatives.

**SEC. 14. AUTHORIZATION OF APPROPRIATIONS.**

(a) **IMPROVEMENTS TO AUTOMATED TARGETING**
**SYSTEM.**—There are authorized to be appropriated
$5,000,000 for each of the fiscal years 2007 through 2012
to carry out the provisions of section 4(b).

(b) **OFFICE OF CARGO SECURITY POLICY.**—There
are authorized to be appropriated for each of the fiscal
years 2007 through 2012—

(1) $4,000,000 to carry out the amendment
made by section 5(a); and
(2) $1,000,000 to carry out the provisions of section 5(b).

(c) Container Security Initiative.—There are authorized to be appropriated $175,000,000 for each of the fiscal years 2007 through 2012 to carry out the provisions of section 8.

(d) Customs-Trade Partnership Against Terrorism.—There are authorized to be appropriated $75,000,000 for each of the fiscal years 2007 through 2012 to carry out the provisions of section 9.

(e) GreenLane Designation.—There are authorized to be appropriated $50,000,000 for each of the fiscal years 2007 through 2012 to carry out the provisions of section 10.

(f) Incident Response.—

(1) In general.—There are authorized to be appropriated $100,000,000 for each of the fiscal years 2007 through 2012 to carry out the provisions of section 11.

(2) Budget analysis.—Not later than 180 days after the date of enactment of this Act, the Secretary shall submit a budget analysis for implementing the provisions of section 11, including additional cost-sharing arrangements with other Federal
departments and other participants involved in the
joint operation centers, to—

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

(B) the Committee on Appropriations of
the Senate;

(C) the Committee on Homeland Security
of the House of Representatives; and

(D) the Committee on Appropriations of
the House of Representatives.

(g) OPERATION SAFE COMMERCE.—There are au-
alyzed to be appropriated $25,000,000 for each of fiscal
years 2007 through 2012 to carry out the provisions of
section 12(e).

(h) PORT SECURITY GRANT PROGRAM.—There are
authorized to be appropriated $400,000,000 for each of
fiscal years 2007 through 2012 to carry out the grant pro-
gram established under section 13.

(i) OTHER PROVISIONS.—There are authorized to be
appropriated such sums as may be necessary for each of
fiscal years 2007 through 2012 to carry out the provisions
of this Act not otherwise provided for under this section.

(j) SOURCE OF FUNDS.—Amounts authorized to be
appropriated under this section shall originate from duties
collected by the Bureau of Customs and Border Protection.