To improve maritime and cargo security through enhanced layered defenses, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 14, 2006

Mr. DANIEL E. LUNGREN of California (for himself, Ms. HARMAN, Mr. PEARCE, Mr. THOMPSON of Mississippi, Mr. BOEHLERT, Ms. LORETTA SANCHEZ of California, Mr. McCaul of Texas, Mr. DICKS, Mr. SOUDER, Mr. HOYER, Ms. HARRIS, Mr. DeFAZIO, Mr. JINDAL, Ms. JACKSON-Lee of Texas, Mr. SHAYS, Mr. LANGEVIN, Mr. DENT, Ms. NORTON, Mr. SIMMONS, Mr. ETHERIDGE, Ms. GINNY BROWN-Waite of Florida, Mr. BROWN of South Carolina, Mr. MEEK of Florida, Mrs. BONO, Mr. LARSEN of Washington, Mr. FERGUSON, Mr. RUPPERSBERGER, Mr. GIBBONS, Mr. SMITH of Washington, Mr. PALLONE, Mr. CARDOZA, Mrs. MALONEY, Mrs. NAPOLITANO, Mr. BROWN of Ohio, Mr. SCHIFF, Mr. BERRY, Ms. EDDIE BERNICE JOHNSON of Texas, Ms. LEE, Ms. KILPATRICK of Michigan, Mr. FORD, Mr. PRICE of North Carolina, Mr. McDERMOTT, Ms. ROYBAL-ALLARD, Mr. BRADY of Pennsylvania, Mr. BISHOP of Georgia, and Mr. Wu) introduced the following bill; which was referred to the Committee on Homeland Security

A BILL

To improve maritime and cargo security through enhanced layered defenses, and for other purposes.

1 Be it enacted by the Senate and House of Representa-
2 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 “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.
Sec. 4. Strategic plan.
Sec. 5. Protocols on the resumption of trade.
Sec. 6. Improvements to Automated Targeting System.
Sec. 7. Uniform data for government-wide usage.
Sec. 8. Employee verification for individuals with access to secure areas of seaports.
Sec. 9. Director of Cargo Security Policy.
Sec. 10. Container security standards and verification procedures.
Sec. 11. Radiation detection and radiation safety.
Sec. 13. Customs-Trade Partnership Against Terrorism.
Sec. 14. GreenLane designation.
Sec. 15. Joint operations centers.
Sec. 16. Research, development, test, and evaluation.
Sec. 17. Port security grant program.
Sec. 18. Authorization of appropriations.

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:

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


(7) 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.

(8) Significant enhancements can be achieved by applying a 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.

(9) 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.

(10) 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” means—
(A) the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives; and

(B) the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate.

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

(3) 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).

(4) 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.

(5) CONTAINER SECURITY INITIATIVE; CSI.—The terms “Container Security Initiative” and “CSI” mean the program authorized under section 12 to identify and examine maritime containers that
pose a risk for terrorism at foreign ports before they are shipped to the United States.

(6) CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM; C–TPAT.—The terms “Customs-Trade Partnership Against Terrorism” and “C–TPAT” mean the voluntary program authorized under section 13 to strengthen and improve the overall security of the international supply chain and United States border security.

(7) DEPARTMENT.—The term “Department” means the Department of Homeland Security.

(8) 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.

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

(10) INSPECTION.—The term “inspection” means the comprehensive process used by U.S. Customs and Border Protection for assessing goods en-
tering the United States to appraise them for duty purposes, to detect the presence of restricted or pro-
hibited items, and to ensure compliance with all ap-
picable laws. This process may include screening,
conducting an examination, or conducting a search.

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

(12) OPERATION SAFE COMMERCE.—The term “Operation Safe Commerce” means the research, de-
velopment, test, and evaluation grant program that brings together private sector shareholders, port offi-
cials, and Federal, State, and local representatives to analyze existing security procedures for cargo and develop new security protocols that have the poten-
tial to increase the security of cargo shipments by monitoring the movement and integrity of cargo through the international supply chain.

(13) 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 ex-
terior packaging unit for movement through the international supply chain.
(14) **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.

(15) **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.

(16) **Secretary.**—The term “Secretary” means the Secretary of Homeland Security.

(17) **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).

(18) **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 container entering the international supply chain.
(19) **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. STRATEGIC PLAN.**

(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 maritime transportation system.

(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 inter-
national supply chain;

(4) provide measurable goals, including objec-
tives, mechanisms, and a schedule, for furthering the
security of commercial operations from point of ori-
gin to point of destination;

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

(6) identify mandatory, baseline security goals,
and the minimum container security standards and
verification procedures described in section 10;

(7) provide incentives for additional voluntary
measures to enhance cargo security, as determined
by the Secretary and under the GreenLane Program
under section 14;

(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 meas-
ured response in the event of a transportation secu-
ity incident involving the international supply chain;

(10) provide a plan for the expeditious resump-
tion of the flow of legitimate trade in accordance
with section 5;
(11) focus on the secure movement of containerized cargo through the international supply chain;
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).

(e) Utilization of Advisory Committees.—As part of the consultations described in subsection (a), 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 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.

(c) Report.—

(1) Initial report.—Not later than 90 days after the date of enactment of this Act, 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.

SEC. 5. PROTOCOLS ON THE 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 ensures trade lanes are restored as quickly as possible. The protocols shall provide for coordination with appropriate Federal, State, and local agencies on law enforcement actions, inter-modal rerouting plans, and identification and prioritization of goods that may enter the United States.
(b) PREFERENCES.—In reestablishing the flow of cargo through ports of entry in the United States after a transportation security incident, the Secretary shall give preference to vessels—

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

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

(3) operated by validated C–TPAT participants;

and

(4) carrying GreenLane designated cargo.

SEC. 6. IMPROVEMENTS TO AUTOMATED TARGETING SYSTEM.

(a) 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 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 implement 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 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, 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;

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

(C) reducing 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.

(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, and the appropriate timing of its submission, 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.

**SEC. 7. UNIFORM DATA FOR GOVERNMENT-WIDE USAGE.**

(a) **ESTABLISHMENT.**—The Secretary, in cooperation with representatives from 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.

(b) Private Sector Consultation.—The Secretary shall consult with private sector stakeholders in developing uniform data submission requirements, procedures, and schedules under the system established pursuant to subsection (a).

SEC. 8. EMPLOYEE VERIFICATION FOR INDIVIDUALS WITH ACCESS TO SECURE AREAS OF SEAPORTS.

(a) Definitions.—In this section, the following definitions apply:

1. **SECRETARY.**—The term “Secretary” means the Secretary of Homeland Security acting through the Assistant Secretary of Homeland Security (Transportation Security Administration).

2. **TERRORIST WATCH LISTS.**—The term “terrorist watch lists” means all available information on known or suspected terrorist threats.

(b) Employee Verification for Current Employees.—
(1) Security directive.—Not later than 30 days after the date of enactment of this Act, the Secretary shall issue a security directive requiring States to submit to the Secretary biographic information on each individual employed, as of the date of issuance of the security directive, in a position in which the individual has access to a secure area of a seaport in the United States.

(2) Determination of secure areas.—The Secretary shall work with the Commandant of the Coast Guard to determine which areas will be treated as secure areas for the purposes of this subsection.

(3) Deadline for submission of information.—The security directive shall require that States submit the biographic information by not later than 30 days after the date of issuance of the security directive.

(4) Comparison of biographic information against information on known or suspected terrorist threats.—

(A) Requirement.—Not later than 75 days after the date of enactment of this Act, the Secretary shall compare the biographic in-
formation received on each individual against terrorist watch lists.

(B) LIMITATION.—The Secretary may omit from any comparison under this subsection information regarding an individual who has previously been compared against terrorist watch lists.

(5) PROCESS.—

(A) MANNER OF COLLECTION AND STORAGE OF INFORMATION.—The Secretary shall determine the manner in which the biographic information will be collected and stored.

(B) COSTS OF COMPARISONS.—The Secretary may not charge any fee for conducting comparisons under this subsection.

(e) EMPLOYEE VERIFICATION FOR FUTURE EMPLOYEES.—

(1) REQUIREMENT.—Not later than 75 days after the date of enactment of this Act, the Secretary shall establish and begin implementing a process for—

(A) obtaining biographic information on individuals employed, beginning after the date of issuance of the security directive under sub-
section (b)(1), in a position described in subsection (b)(1); and

(B) comparing the biographic information
on such individuals against all available infor-
mation on known or suspected terrorist threats.

(2) Costs of Comparisons.—The Secretary
shall determine how to cover costs of comparisons
conducted pursuant to this subsection.

(d) Prohibited Employment.—The Secretary
shall specify security factors that are sufficient to prohibit
the employment of an individual in a position described
in subsection (b)(1).

(e) Protections for Individuals.—The Secretary
shall issue regulations to establish protections for individ-
uals subject to comparisons under this section. The protec-
tions shall be substantially equivalent to the protections
for individuals under sections 70105(c)(2), 70105(c)(3),
and 70105(e) of title 46, United States Code.

(f) Restrictions on Use and Maintenance of
Information.—

(1) Restriction on disclosure.—Information
obtained by the Secretary on an individual
under this section may not be made available to the
public, including the individual’s employer.
(2) CONFIDENTIALITY; USE.—Any information constituting grounds for prohibiting the employment of an individual in a position described in subsection (b)(1) 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 other Federal law enforcement agencies. The Secretary may not share any such information with an individual’s employer, except to inform the employer of whether or not the individual has been prohibited under this section from employment in a position described in subsection (b)(1).

(g) REPORTING.—Not later than 90 days after the date of enactment of this Act, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Reform of the Senate a report containing information on—

(1) the number of matches made in conducting comparisons under subsection (b); and

(2) the corresponding ports at which the matches were identified; and
(3) the actions taken to determine necessary corrective actions, as well as any corrective actions taken.

SEC. 9. DIRECTOR OF CARGO SECURITY POLICY.

(a) IN GENERAL.—There shall be in the Department a Director of Cargo Security Policy (hereinafter in this section referred to as the “Director”).

(b) RESPONSIBILITIES.—The Director shall—

(1) advise the Secretary regarding all aspects of Department programs relating to cargo security;

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

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

SEC. 10. CONTAINER SECURITY STANDARDS AND VERIFICATION 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 verification procedures for securing con-
tainers 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 15.
(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. 11. Radiation Detection and Radiation Safety.**

(a) **Strategy.**—Not later than 90 days after the date of 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 radiation detection equipment at all ports of entry.

(b) **Contents.**—The strategy submitted under subsection (a) shall include—

1. A risk-based prioritization of maritime ports of entry at which radiation detection equipment will be deployed;

2. A proposed timeline of when radiation detection equipment will be deployed at each of the maritime ports of entry identified under paragraph (1);
(3) the type of equipment to be used at each of
the maritime ports of entry identified under para-
graph (1);

(4) standard operating procedures for exam-
ing containers with such equipment;

(5) an evaluation of the environmental health
and safety impacts of nonintrusive inspection tech-
nology;

(6) the Department policy for using nonintru-
sive inspection equipment;

(7) a classified annex that details plans for cov-
ert testing;

(8) a classified annex that outlines the risk-
based prioritization of maritime ports of entry used
under paragraph (1); and

(9) a plan that—

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

(B) describes the policy of U.S. Customs
and Border Protection for using nonintrusive
inspection equipment.

SEC. 12. 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 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; and

(6) 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 to the appropriate congressional committees a report, in classified or unclassified form, detailing the assessment of each foreign port the Secretary is considering designating under CSI.

(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 (c) that includes that port.

(f) 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 consultation 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 designated under CSI and foreign ports not designated under CSI that lack effective antiterrorism measures.

(B) ACQUISITION.—The Secretary may lease, loan, or otherwise provide foreign authorities nonintrusive inspection equipment or radiation detection equipment for examining conveyances and intermodal shipping containers at any foreign or domestic port, under such terms and conditions the Secretary may determine (including nonreimbursable transfer of ownership), if provision of such equipment is determined by the Secretary to help secure and
facilitate international trade and is in the interests of the United States.

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

(g) 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 to decrease the number of personnel who are deployed at foreign ports.

SEC. 13. 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 the overall security of the international supply chain and United States border security.

(2) GAO RECOMMENDATIONS.—The Secretary shall address, and to the extent appropriate imple-
ment, the recommendations of the C–TPAT program that were identified in the Government Accountability Office report entitled “CARGO SECURITY: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security” (GAO–05–404).

(3) MINIMUM REQUIREMENTS.—The Secretary shall establish minimum 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 Department.

(c) 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.

(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 secu-

rity 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).

(e) 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, the Commissioner of U.S. Customs and Border Protection may—

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

or

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

(4) RIGHT OF APPEAL.—A C–TPAT participant described under paragraph (3) may file an appeal with the Secretary of the Commissioner’s decision under paragraph (3)(A) to deny benefits under C–TPAT and under paragraph (3)(B) to suspend or expel the participant from C–TPAT.
(5) Tier Two Benefits.—The Secretary shall extend benefits to each participant who has been validated under this subsection, which may include—

(A) reduced examinations; and

(B) priority processing for searches.

(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. 14. 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 on a vessel with a vessel security plan approved or accepted under section 70103(e) of title 46, United States Code, or the International Ship and Port Facility (ISPS) Code;
(3) container security devices that exceed the standards and procedures established by the Secretary are utilized;

(4) cargo security practices exceed the security criteria established by the Secretary beyond the minimum requirements for C–TPAT participation under section 13(c), particularly in the area of access controls; and

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

(c) CONTAINERS TRANSHIPPEP 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) Policies.—

(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 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 requirements that the Secretary considers appropriate, including requirements building upon security measures and supply chain security best
practices contained in the C–TPAT minimum requirements set forth in section 13(e).

(2) BENEFITS.—Not later than 2 years after the date of enactment of this Act, the Secretary, in consultation with the Commercial Operations Advisory Committee, may provide 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 requirements for GreenLane cargo;

(C) preference to vessels (as described in section 5(b));

(D) further reduced examinations;

(E) priority processing for examinations;

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

(G) streamlined billing of any customs duties or fees.
SEC. 15. JOINT OPERATIONS CENTERS.

(a) Establishment.—Not later than three years after the date of the enactment of this Act, the Secretary shall expand existing and establish new joint operations 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) Participation.—The following entities shall participate in each joint operations center for maritime and cargo security:

(1) The United States Coast Guard.

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

(3) U.S. 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.

(c) 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 (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 of such title 46, United States Code; and

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

(d) 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.

(e) 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.

(f) IMPLEMENTATION.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary shall submit to the appropriate congressional committees an implementation plan for this section.

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

(A) the location;

(B) the specific participating entities;

(C) the implementation costs;

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

(E) in the case of an existing joint operations center, the enhancements to such center that are necessary to meet the requirements of subsection (d).

SEC. 16. RESEARCH, DEVELOPMENT, TEST, AND EVALUATION.

(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, acting through the Undersecretary for Science and Technology, in consultation with the Assistant Secretary for Policy, the Director of Cargo Security Policy, the Director of the Domestic Nuclear Detection Office of the Department, 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.

(c) 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 to include continuous tracking devices that provide real-time monitoring and reporting;

(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 to the appropriate congressional committees a report detailing the results of Operation Safe Commerce.

(d) GreenLane technology.—The Secretary shall, not less frequently than once every 2 years—

(1) review the technology requirements and standards established under section 14; and

(2) test future supply chain visibility procedures, container security devices, and other systems as they become commercially available to track and secure containers and the smallest exterior packaging units loaded into containers.

SEC. 17. PORT SECURITY GRANT PROGRAM.

(a) Grants authorized.—The Secretary shall establish a grant program to allocate Federal financial as-
istance to ports in the United States on the basis of risk and need.

(b) PRIORITIZATION PROCESS.—In awarding grants under this section, the Secretary shall conduct an assessment of ports in the United States 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.

(e) APPLICATION.—

(1) IN GENERAL.—Any entity subject to an Area Maritime Transportation Security Plan required under section 70103(b) 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 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 identified by the Coast Guard, or through port security vulner-
ability assessments approved by the Secretary; 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 port or a system of ports in the United States, 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 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;

(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 Security Plan, if the need is based upon vulnerability assessments approved by the Sec-
retary 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 to strengthen terrorism preparedness;

(9) to conduct training for prevention and detection of, preparedness for, response to, or recovery from attacks involving weapons of mass destruction, including training in the use of equipment and computer software;

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

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

(12) 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

(13) 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, acquire land; or

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

(f) MULTIPLE PHASE PROJECTS.—

(1) SENSE OF CONGRESS.—It is the sense of Congress that the Secretary should consider awarding 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.

(g) 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 used to supplement and support any applicable State or Urban Area Homeland Security Plan.

(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
3 SEC. 18. 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 6.

(b) CONTAINER SECURITY INITIATIVE.—There are authorized to be appropriated $196,000,000 for each of the fiscal years 2007 through 2012 to carry out the provisions of section 12.

(c) 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 sections 13 and 14.

(d) JOINT OPERATIONS CENTERS.—

(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 15.

(2) BUDGET ANALYSIS.—Not later than 180 days after the date of enactment of this Act, the Secretary shall submit to the appropriate congressional committees a budget analysis for implementing the provisions of section 15, including addi-
tional cost-sharing arrangements with other Federal
departments and other participants involved in the
joint operation centers.
(e) Operation Safe Commerce.—There are au-

thorized to be appropriated $25,000,000 for each of fiscal
years 2007 through 2012 to carry out the provisions of
section 16(e).
(f) Port Security Grant Program.—
(1) In general.—There are authorized to be
appropriated $400,000,000 for each of fiscal years
2007 through 2012 to carry out the grant program
established under section 17.
(2) Source of funds.—Amounts authorized
to be appropriated under paragraph (1) shall origi-
nate from duties collected by U.S. Customs and Bor-
der Protection.
(g) 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.