

## **Security and Accountability For Every Port Act of 2006**

[Public Law 109–347; Approved October 13, 2006]

[As Amended Through P.L. 115–254, Enacted October 5, 2018]

【Currency: This publication is a compilation of the text of Public Law 109-347. It was last amended by the public law listed in the As Amended Through note above and below at the bottom of each page of the pdf version and reflects current law through the date of the enactment of the public law listed at <https://www.govinfo.gov/app/collection/comps/>】

【Note: While this publication does not represent an official version of any Federal statute, substantial efforts have been made to ensure the accuracy of its contents. The official version of Federal law is found in the United States Statutes at Large and in the United States Code. The legal effect to be given to the Statutes at Large and the United States Code is established by statute (1 U.S.C. 112, 204).】

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

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

### **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

(a) 【 6 U.S.C. 901 note】 **SHORT TITLE.**—This Act may be cited as the “Security and Accountability For Every Port Act of 2006” or the “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. Definitions.

### **TITLE I—SECURITY OF UNITED STATES SEAPORTS**

#### **Subtitle A—General Provisions**

- Sec. 101. Area Maritime Transportation Security Plan to include salvage response plan.
- Sec. 102. Requirements relating to maritime facility security plans.
- Sec. 103. Unannounced inspections of maritime facilities.
- Sec. 104. Transportation security card.
- [Sec. 105. Repealed.]
- Sec. 106. Prohibition of issuance of transportation security cards to persons convicted of certain felonies.
- Sec. 107. Long-range vessel tracking.
- Sec. 108. Establishment of interagency operational centers for port security.
- Sec. 109. Notice of arrival for foreign vessels on the Outer Continental Shelf.
- Sec. 110. Enhanced crewmember identification.

#### **Subtitle B—Port Security Grants; Training and Exercise Programs**

- Sec. 111. Risk assessment tool.
- Sec. 112. Port security grants.
- Sec. 113. Port Security Training Program.
- Sec. 114. Port Security Exercise Program.
- Sec. 115. Facility exercise requirements.

**Sec. 1                      Security and Accountability For Every Port Act of...                      2**

Subtitle C—Port Operations

- Sec. 121. Domestic radiation detection and imaging.
- [Sec. 122. Repealed.]
- Sec. 123. Random searches of containers.
- Sec. 124. Work stoppages and employee-employer disputes.
- Sec. 125. Threat assessment screening of port truck drivers.
- Sec. 126. Border Patrol unit for United States Virgin Islands.
- [Sec. 127. Repealed.]
- Sec. 128. Center of Excellence for Maritime Domain Awareness.

**TITLE II—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN**

Subtitle A—General Provisions

- Sec. 201. Strategic plan to enhance the security of the international supply chain.
- Sec. 202. Post-incident resumption of trade.
- Sec. 203. Automated Targeting System.
- Sec. 204. Container security standards and procedures.
- Sec. 205. Container Security Initiative.

Subtitle B—Customs-Trade Partnership Against Terrorism

- Sec. 211. Establishment.
- Sec. 212. Eligible entities.
- Sec. 213. Minimum requirements.
- Sec. 214. Tier 1 participants in C-TPAT.
- Sec. 215. Tier 2 participants in C-TPAT.
- Sec. 216. Tier 3 participants in C-TPAT.
- Sec. 217. Consequences for lack of compliance.
- Sec. 218. Third party validations.
- Sec. 219. Revalidation.
- Sec. 220. Noncontainerized cargo.
- Sec. 221. C-TPAT program management.
- Sec. 222. Additional personnel.
- Sec. 223. Authorization of appropriations.

Subtitle C—Miscellaneous Provisions

- Sec. 231. Pilot integrated scanning system.
- Sec. 232. Screening and scanning of cargo containers.
- Sec. 233. Inspection technology and training.
- Sec. 234. Foreign port assessments.
- [Sec. 235. Repealed.]
- Sec. 236. Information sharing relating to supply chain security cooperation.

**TITLE III—ADMINISTRATION**

- Sec. 301. Office of Cargo Security Policy.
- Sec. 302. Reauthorization of Homeland Security Science and Technology Advisory Committee.
- Sec. 303. Research, development, test, and evaluation efforts in furtherance of maritime and cargo security.

**TITLE IV—AGENCY RESOURCES AND OVERSIGHT**

- Sec. 401. Trade and customs revenue functions of the department.
- Sec. 402. Office of international trade; oversight.
- Sec. 403. Resources.
- Sec. 404. Negotiations.
- Sec. 405. International Trade Data System.
- Sec. 406. In-bond cargo.
- Sec. 407. Sense of the Senate.

**TITLE V—DOMESTIC NUCLEAR DETECTION OFFICE**

- Sec. 501. Establishment of Domestic Nuclear Detection Office.
- Sec. 502. Technology research and development investment strategy for nuclear and radiological detection.

**TITLE VI—COMMERCIAL MOBILE SERVICE ALERTS**

- Sec. 601. Short title.
- Sec. 602. Federal Communications Commission duties.

Sec. 603. Commercial Mobile Service Alert Advisory Committee.  
 Sec. 604. Research and development.  
 Sec. 605. Grant program for remote community alert systems.  
 Sec. 606. Funding.  
 Sec. 607. Essential services disaster assistance.  
 Sec. 608. Community disaster loans.  
 Sec. 609. Public facilities.  
 Sec. 610. Expedited payments.  
 Sec. 611. Use of local contracting.  
 Sec. 612. FEMA programs.  
 Sec. 613. Homeland security definition.

## TITLE VII—OTHER MATTERS

[Sec. 701. Repealed.]  
 Sec. 702. Disclosures regarding homeland security grants.  
 Sec. 703. Trucking security.  
 Sec. 704. Air and Marine Operations of the Northern Border Air Wing.  
 Sec. 705. Phaseout of vessels supporting oil and gas development.  
 Sec. 706. Coast Guard property in Portland, Maine.  
 Sec. 707. Methamphetamine and methamphetamine precursor chemicals.  
 [Sec. 708. Repealed.]  
 Sec. 709. Protection of health and safety during disasters.

## TITLE VIII—UNLAWFUL INTERNET GAMBLING ENFORCEMENT

Sec. 801. Short title.  
 Sec. 802. Prohibition on acceptance of any payment instrument for unlawful Internet gambling.  
 Sec. 803. Internet gambling in or through foreign jurisdictions.

**SEC. 2. [6 U.S.C. 901] DEFINITIONS.**

In this Act:

(1) **APPROPRIATE CONGRESSIONAL COMMITTEES.**—Except as otherwise provided, the term “appropriate congressional committees” means—

- (A) the Committee on Appropriations of the Senate;
- (B) the Committee on Commerce, Science, and Transportation of the Senate;
- (C) the Committee on Finance of the Senate;
- (D) the Committee on Homeland Security and Governmental Affairs of the Senate;
- (E) the Committee on Appropriations of the House of Representatives;
- (F) the Committee on Homeland Security of the House of Representatives;
- (G) the Committee on Transportation and Infrastructure of the House of Representatives;
- (H) the Committee on Ways and Means of the House of Representatives; and
- (I) other congressional committees, as appropriate.

(2) **COMMERCIAL OPERATIONS ADVISORY COMMITTEE.**—The term “Commercial Operations Advisory Committee” means the Advisory Committee established pursuant to section 9503(c) of the Omnibus Budget Reconciliation Act of 1987 (19 U.S.C. 2071 note) or any successor committee.

(3) **COMMERCIAL SEAPORT PERSONNEL.**—The term “commercial seaport personnel” includes any person engaged in an activity relating to the loading or unloading of cargo or passengers, the movement or tracking of cargo, the maintenance and repair of intermodal equipment, the operation of cargo-related equipment (whether or not integral to the vessel), and

the handling of mooring lines on the dock when a vessel is made fast or let go in the United States.

(4) COMMISSIONER.—The term “Commissioner” means the Commissioner responsible for the United States Customs and Border Protection of the Department of Homeland Security.

(5) 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).

(6) CONTAINER SECURITY DEVICE.—The term “container security device” means a device, or system, designed, at a minimum, to identify positively a container, to detect and record the unauthorized intrusion of a container, and to secure a container against tampering throughout the supply chain. Such a device, or system, shall have a low false alarm rate as determined by the Secretary.

(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 that utilizes nonintrusive imaging and detection technology.

(9) INSPECTION.—The term “inspection” means the comprehensive process used by the United States Customs and Border Protection to assess goods entering the United States to appraise them for duty purposes, to detect the presence of restricted or prohibited items, and to ensure compliance with all applicable laws. The 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 to or from the United States beginning at the point of origin (including manufacturer, supplier, or vendor) through a point of distribution to the destination.

(11) RADIATION DETECTION EQUIPMENT.—The term “radiation detection equipment” means any technology that is capable of detecting or identifying nuclear and radiological material or nuclear and radiological explosive devices.

(12) SCAN.—The term “scan” means utilizing nonintrusive imaging equipment, radiation detection equipment, or both, to capture data, including images of a container.

(13) 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 the presence of misdeclared, restricted, or prohibited items and assess the level of threat posed by such cargo.

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

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

(16) **TRANSPORTATION DISRUPTION.**—The term “transportation disruption” means any significant delay, interruption, or stoppage in the flow of trade caused by a natural disaster, heightened threat level, an act of terrorism, or any transportation security incident (as defined in section 70101(6) of title 46, United States Code).

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

## **TITLE I—SECURITY OF UNITED STATES SEAPORTS**

### **Subtitle A—General Provisions**

\* \* \* \* \*

#### **SEC. 108. ESTABLISHMENT OF INTERAGENCY OPERATIONAL CENTERS FOR PORT SECURITY.**

(a) **IN GENERAL.**—Chapter 701 of title 46, United States Code, is amended by inserting after section 70107 the following:

**“SEC. 70107A. Interagency operational centers for port security**

“(a) **IN GENERAL.**—The Secretary shall establish interagency operational centers for port security at all high-priority ports not later than 3 years after the date of the enactment of the SAFE Port Act.

“(b) **CHARACTERISTICS.**—The interagency operational centers established under this section shall—

“(1) utilize, as appropriate, the compositional and operational characteristics of existing centers, including—

“(A) the pilot project interagency operational centers for port security in Miami, Florida; Norfolk/Hampton Roads, Virginia; Charleston, South Carolina; and San Diego, California; and

“(B) the virtual operation center of the Port of New York and New Jersey;

“(2) be organized to fit the security needs, requirements, and resources of the individual port area at which each is operating;

“(3) in addition to the Coast Guard, provide, as the Secretary determines appropriate, for participation by representatives of the United States Customs and Border Protection, the United States Immigration and Customs Enforcement, the Transportation Security Administration, the Department of Justice, the Department of Defense, and other Federal agencies, State and local law enforcement or port security personnel, members of the Area Maritime Security Committee, and other public and private sector stakeholders adversely affected by a transportation security incident or transportation disruption; and

“(4) be incorporated in the implementation and administration of—

“(A) maritime transportation security plans developed under section 70103;

“(B) maritime intelligence activities under section 70113 and information sharing activities consistent with 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.);

“(C) short- and long-range vessel tracking under sections 70114 and 70115;

“(D) protocols under section 201(b)(10) of the SAFE Port Act;

“(E) the transportation security incident response plans required by section 70104; and

“(F) other activities, as determined by the Secretary.

“(c) SECURITY CLEARANCES.—The Secretary shall sponsor and expedite individuals participating in interagency operational centers in gaining or maintaining their security clearances. Through the Captain of the Port, the Secretary may identify key individuals who should participate. The port or other entities may appeal to the Captain of the Port for sponsorship.

“(d) SECURITY INCIDENTS.—During a transportation security incident on or adjacent to waters subject to the jurisdiction of the United States, the Coast Guard Captain of the Port designated by the Commandant of the Coast Guard in a maritime security command center described in subsection (a) shall act as the incident commander, unless otherwise directed by the President.

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

“(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated \$60,000,000 for each of the fiscal years 2007 through 2012 to carry out this section.”.

(b) [46 U.S.C. 70107A note] [Reserved].<sup>1</sup>

(c) BUDGET AND COST-SHARING ANALYSIS.—Not later than 180 days after the date of the enactment of this Act, the Secretary of the department in which the Coast Guard is operating shall submit to the appropriate congressional committees a proposed budget analysis for implementing section 70107A of title 46, United States Code, as added by subsection (a), including cost-sharing arrangements with other Federal departments and agencies involved in the interagency operation of the centers to be established under such section.

(d) CLERICAL AMENDMENT.—The chapter analysis for chapter 701 of title 46, United States Code, is amended by inserting after the item relating to section 70107 the following:

“70107A. Interagency operational centers for port security”.

\* \* \* \* \*

<sup>1</sup> Subsection (b) of section 108 as it appears above is so in law pursuant to section 1809(c)(2) of division J of Public Law 115–254 (132 Stat. 3538).

## Subtitle C—Port Operations

### SEC. 121. [6 U.S.C. 921] DOMESTIC RADIATION DETECTION AND IMAGING.

(a) SCANNING CONTAINERS.—Subject to section 1318 of title 19, United States Code, not later than December 31, 2007, all containers entering the United States through the 22 ports through which the greatest volume of containers enter the United States by vessel shall be scanned for radiation. To the extent practicable, the Secretary shall deploy next generation radiation detection technology.

(b) STRATEGY.—The Secretary shall develop a strategy for the deployment of radiation detection capabilities that includes—

(1) a risk-based prioritization of 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 port of entry identified under paragraph (1);

(3) the type of equipment to be used at each port of entry identified under paragraph (1), including the joint deployment and utilization of radiation detection equipment and nonintrusive imaging equipment;

(4) standard operating procedures for examining containers with such equipment, including sensor alarming, networking, and communications and response protocols;

(5) operator training plans;

(6) an evaluation of the environmental health and safety impacts of nonintrusive imaging technology and a radiation risk reduction plan, in consultation with the Nuclear Regulatory Commission, the Occupational Safety and Health Administration, and the National Institute for Occupational Safety and Health, that seeks to minimize radiation exposure of workers and the public to levels as low as reasonably achievable;

(7) the policy of the Department for using nonintrusive imaging equipment in tandem with radiation detection equipment; and

(8) a classified annex that—

(A) details plans for covert testing; and

(B) outlines the risk-based prioritization of ports of entry identified under paragraph (1).

(c) STANDARDS.—The Secretary, acting through the Director for Domestic Nuclear Detection and in collaboration with the National Institute of Standards and Technology, shall publish technical capability standards and recommended standard operating procedures for the use of nonintrusive imaging and radiation detection equipment in the United States. Such standards and procedures—

(1) should take into account relevant standards and procedures utilized by other Federal departments or agencies as well as those developed by international bodies; and

(2) shall not be designed so as to endorse specific companies or create sovereignty conflicts with participating countries.

(d) IMPLEMENTATION.—Not later than 3 years after the date of the enactment of this Act, the Secretary shall fully implement the strategy developed under subsection (b).

(e) EXPANSION TO OTHER UNITED STATES PORTS OF ENTRY.—

(1) IN GENERAL.—As soon as practicable after—

(A) implementation of the program for the examination of containers for radiation at ports of entry described in subsection (a); and

(B) submission of the strategy developed under subsection (b),

but not later than December 31, 2008, the Secretary shall expand the strategy developed under subsection (b), in a manner consistent with the requirements of subsection (b), to provide for the deployment of radiation detection capabilities at all other United States ports of entry not covered by the strategy developed under subsection (b).

(2) RISK ASSESSMENT.—In expanding the strategy under paragraph (1), the Secretary shall identify and assess the risks to those other ports of entry in order to determine what equipment and practices will best mitigate the risks.

(f) INTERMODAL RAIL RADIATION DETECTION TEST CENTER.—

(1) ESTABLISHMENT.—In accordance with subsection (b), and in order to comply with this section, the Secretary shall establish an Intermodal Rail Radiation Detection Test Center (referred to in this subsection as the “Test Center”).

(2) PROJECTS.—The Secretary shall conduct multiple, concurrent projects at the Test Center to rapidly identify and test concepts specific to the challenges posed by on-dock rail.

(3) LOCATION.—The Test Center shall be located within a public port facility at which a majority of the containerized cargo is directly laden from (or unladen to) on-dock, intermodal rail.

\* \* \* \* \*

## TITLE II—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN

### Subtitle A—General Provisions

#### SEC. 201. [6 U.S.C. 941] STRATEGIC PLAN TO ENHANCE THE SECURITY OF THE INTERNATIONAL SUPPLY CHAIN.

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

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

(1) describe the roles, responsibilities, and authorities of Federal, State, local, and tribal government agencies and pri-



vate-sector stakeholders that relate to the security of the movement of containers through the international supply chain;

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

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

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

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

(6) provide incentives for additional voluntary measures to enhance cargo security, as recommended by the Commissioner;

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

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

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

(10) provide protocols for the expeditious resumption of the flow of trade in accordance with section 202;

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

(12) expand upon and relate to existing strategies and plans, including the National Response Plan, the National Maritime Transportation Security Plan, the National Strategy for Maritime Security, and the 8 supporting plans of the Strategy, as required by Homeland Security Presidential Directive 13.

(c) CONSULTATION.—In developing protocols under subsection (b)(10), the Secretary shall consult with Federal, State, local, and private sector stakeholders, including the National Maritime Security Advisory Committee and the Commercial Operations Advisory Committee.

(d) COMMUNICATION.—To the extent practicable, the strategic plan developed under subsection (a) shall provide for coordination with, and lines of communication among, appropriate Federal, State, local, and private-sector stakeholders on law enforcement actions, intermodal rerouting plans, and other strategic infrastructure issues resulting from a transportation security incident or transportation disruption.

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

(f) **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.

(g) **REPORTS.**—

(1) **INITIAL REPORT.**—Not later than 270 days after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees a report that contains the strategic plan required by subsection (a).

(2) **UPDATES.**—Not later than 270 days after the date of enactment of the Maritime Security Improvement Act of 2018 and triennially thereafter, the Secretary shall submit to the appropriate congressional committees a report that contains any updates to the strategic plan under subsection (a) since the prior report.

**SEC. 202. [6 U.S.C. 942] POST-INCIDENT RESUMPTION OF TRADE.**

(a) **IN GENERAL.**—The Secretary shall develop and update, as necessary, protocols for the resumption of trade in accordance with section 201(b)(10) in the event of a transportation disruption or a transportation security incident. The protocols shall include—

(1) the identification of the appropriate initial incident commander, if the Commandant of the Coast Guard is not the appropriate person, and lead departments, agencies, or offices to execute such protocols;

(2) a plan to redeploy resources and personnel, as necessary, to reestablish the flow of trade;

(3) a plan to provide training for the periodic instruction of personnel of the United States Customs and Border Protection, the Coast Guard, and the Transportation Security Administration in trade resumption functions and responsibilities; and

(4) appropriate factors for establishing prioritization of vessels and cargo determined by the President to be critical for response and recovery, including factors relating to public health, national security, and economic need.

(b) **VESSELS.**—In determining the prioritization of vessels accessing facilities (as defined under section 70101 of title 46, United States Code), the Commandant of the Coast Guard may, to the extent practicable and consistent with the protocols and plans required under this section to ensure the safe and secure transit of vessels to ports in the United States after a transportation security incident, give priority to a vessel—

(1) that has an approved security plan under section 70103(c) of title 46, United States Code, or a valid international ship security certificate, as provided under part 104 of title 33, Code of Federal Regulations;

(2) that is manned by individuals who are described in section 70105(b)(2)(B) of title 46, United States Code; and

(3) that is operated by validated participants in the Customs-Trade Partnership Against Terrorism program.

(c) CARGO.—In determining the prioritization of the resumption of the flow of cargo and consistent with the protocols established under this section, the Commissioner may give preference to cargo—

(1) entering a port of entry directly from a foreign seaport designated under the Container Security Initiative;

(2) from the supply chain of a validated C-TPAT participant and other private sector entities, as appropriate; or

(3) that has undergone—

(A) a nuclear or radiological detection scan;

(B) an x-ray, density, or other imaging scan; and

(C) a system to positively identify the container at the last port of departure prior to arrival in the United States, which data has been evaluated and analyzed by personnel of the United States Customs and Border Protection.

(d) COORDINATION.—The Secretary shall ensure that there is appropriate coordination among the Commandant of the Coast Guard, the Commissioner, and other Federal officials following a maritime disruption or maritime transportation security incident in order to provide for the resumption of trade.

(e) COMMUNICATION.—Consistent with section 201, the Commandant of the Coast Guard, Commissioner, and other appropriate Federal officials, shall promptly communicate any revised procedures or instructions intended for the private sector following a maritime disruption or maritime transportation security incident.

**SEC. 203. [6 U.S.C. 943] AUTOMATED TARGETING SYSTEM.**

(a) IN GENERAL.—The Secretary, acting through the Commissioner, shall—

(1) identify and seek the submission of data related to the movement of a shipment of cargo through the international supply chain; and

(2) analyze the data described in paragraph (1) to identify high-risk cargo for inspection.

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

(c) CONSIDERATION.—The Secretary, acting through the Commissioner, shall—

(1) consider the cost, benefit, and feasibility of—

(A) requiring additional nonmanifest documentation;

(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 certain elements 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 successor targeting system in furthering the security and integrity of the international supply chain; and

(2) consult with stakeholders, including the Commercial Operations Advisory Committee, and identify to them the need for such information, and the appropriate timing of its submission.

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

(e) SYSTEM IMPROVEMENTS.—The Secretary, acting through the Commissioner, shall—

(1) conduct, through an independent panel, a review of the effectiveness and capabilities of the Automated Targeting System;

(2) 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) ensure that the Automated Targeting System has the capability to electronically compare manifest and other available data for cargo entered into or bound for the United States to detect any significant anomalies between such data and facilitate the resolution of such anomalies;

(4) ensure that the Automated Targeting System has the capability to electronically identify, compile, and compare select data elements for cargo entered into or bound for the United States following a maritime transportation security incident, in order to efficiently identify cargo for increased inspection or expeditious release; and

(5) develop a schedule to address the recommendations of the Comptroller General of the United States, the Inspector General of the Department of the Treasury, and the Inspector General of the Department with respect to the operation of the Automated Targeting System.

(f) 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.

(g) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the United States Customs and Border Protection to carry out the Automated Targeting System for identifying high-risk oceanborne container cargo for inspection—

(1) \$33,200,000 for fiscal year 2008;

(2) \$35,700,000 for fiscal year 2009; and

(3) \$37,485,000 for fiscal year 2010.

#### SEC. 204. [6 U.S.C. 944] CONTAINER SECURITY STANDARDS AND PROCEDURES.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall initiate a rule-making proceeding to establish minimum standards and procedures for securing containers in transit to the United States.

(2) INTERIM RULE.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall issue an interim final rule pursuant to the proceeding described in paragraph (1).

(3) MISSED DEADLINE.—If the Secretary is unable to meet the deadline established pursuant to paragraph (2), the Secretary shall submit a letter to the appropriate congressional committees explaining why the Secretary is unable to meet that deadline and describing what must be done before such minimum standards and procedures can be established.

(4) DEADLINE FOR ENFORCEMENT.—

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

(B) INTERIM REQUIREMENT.—If the interim final rule described in paragraph (2) is not issued by April 1, 2008, then—

(i) effective not later than October 15, 2008, all containers in transit to the United States shall be required to meet the requirements of International Organization for Standardization Publicly Available Specification 17712 standard for sealing containers; and

(ii) the requirements of this subparagraph shall cease to be effective upon the effective date of the interim final rule issued pursuant to this subsection.

(b) REVIEW AND ENHANCEMENT.—The Secretary shall regularly review and enhance the standards and procedures established pursuant to subsection (a), as appropriate, based on tests of technologies as they become commercially available to detect container intrusion and the highest consequence threats, particularly weapons of mass destruction.

(c) INTERNATIONAL CARGO SECURITY STANDARDS.—The Secretary, in consultation with the Secretary of State, the Secretary of Energy, and other Federal Government officials, as appropriate, and with the Commercial Operations Advisory Committee, the Homeland Security Advisory Committee, and the National Maritime Security Advisory Committee, 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, the International Organization for Standardization, the International Labor Organization, and the World Customs Organization.

(d) INTERNATIONAL TRADE AND OTHER OBLIGATIONS.—In carrying out this section, the Secretary shall consult with appropriate Federal departments and agencies and private sector stakeholders and ensure that actions under this section do not violate inter-

national trade obligations or other international obligations of the United States.

**SEC. 205. [6 U.S.C. 945] CONTAINER SECURITY INITIATIVE.**

(a) **ESTABLISHMENT.**—The Secretary, acting through the Commissioner, shall establish and implement a program (referred to in this section as the “Container Security Initiative” or “CSI”) to identify and examine or search maritime containers that pose a security risk before loading such containers in a foreign port for shipment to the United States, either directly or through a foreign port.

(b) **ASSESSMENT.**—The Secretary, acting through the Commissioner, may designate foreign seaports to participate in the Container Security Initiative after the Secretary has assessed the costs, benefits, and other factors associated with such designation, including—

(1) the level of risk for the potential compromise of containers by terrorists, or other threats as determined by the Secretary;

(2) the volume of cargo being imported to the United States directly from, or being transshipped through, the foreign seaport;

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

(4) the commitment of the government of the country in which the foreign seaport is located to cooperating with the Department in sharing critical data and risk management information and to maintain programs to ensure employee integrity; and

(5) the potential for validation of security practices at the foreign seaport by the Department.

(c) **NOTIFICATION.**—The Secretary shall notify the appropriate congressional committees of the designation of a foreign port under the Container Security Initiative or the revocation of such a designation before notifying the public of such designation or revocation.

(d) **NEGOTIATIONS.**—The Secretary, in cooperation with the Secretary of State and in consultation with the United States Trade Representative, may enter into negotiations with the government of each foreign nation in which a seaport is designated under the Container Security Initiative to ensure full compliance with the requirements under the Container Security Initiative.

(e) **OVERSEAS INSPECTIONS.**—

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

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

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

(C) continually monitor the technologies, processes, and techniques used to inspect cargo at ports designated under CSI to ensure adherence to such criteria and the use of such procedures; and

(D) consult with the Secretary of Energy in establishing the minimum technical capability criteria and standard operating procedures established under subparagraph (A) pertaining to radiation detection technologies to promote consistency in detection systems at foreign ports designated under CSI.

(2) CONSTRAINTS.—The criteria and procedures established under paragraph (1)(A)—

(A) shall be consistent, as practicable, with relevant standards and procedures utilized by other Federal departments or agencies, or developed by international bodies if the United States consents to such standards and procedures;

(B) shall not apply to activities conducted under the Megaports Initiative of the Department of Energy; and

(C) shall not be designed to endorse the product or technology of any specific company or to conflict with the sovereignty of a country in which a foreign seaport designated under the Container Security Initiative is located.

(f) SAVINGS PROVISION.—The authority of the Secretary under this section shall not affect any authority or duplicate any efforts or responsibilities of the Federal Government with respect to the deployment of radiation detection equipment outside of the United States.

(g) COORDINATION.—The Secretary shall—

(1) coordinate with the Secretary of Energy, as necessary, to provide radiation detection equipment required to support the Container Security Initiative through the Department of Energy's Second Line of Defense Program and Megaports Initiative; or

(2) work with the private sector or host governments, when possible, to obtain radiation detection equipment that meets the Department's and the Department of Energy's technical specifications for such equipment.

(h) STAFFING.—The Secretary shall develop a human capital management plan to determine adequate staffing levels in the United States and in foreign seaports including, as appropriate, the remote location of personnel in countries in which foreign seaports are designated under the Container Security Initiative.

(i) ANNUAL DISCUSSIONS.—The Secretary, in coordination with the appropriate Federal officials, shall hold annual discussions with foreign governments of countries in which foreign seaports designated under the Container Security Initiative are located regarding best practices, technical assistance, training needs, and technological developments that will assist in ensuring the efficient and secure movement of international cargo.

(j) LESSER RISK PORT.—The Secretary, acting through the Commissioner, may treat cargo loaded in a foreign seaport designated under the Container Security Initiative as presenting a lesser risk than similar cargo loaded in a foreign seaport that is not

designated under the Container Security Initiative, for the purpose of clearing such cargo into the United States.

(k) PROHIBITION.—

(1) IN GENERAL.—The Secretary shall issue a “do not load” order, using existing authorities, to prevent the onload of any cargo loaded at a port designated under CSI that has been identified as high risk, including by the Automated Targeting System, unless the cargo is determined to no longer be high risk through—

(A) a scan of the cargo with nonintrusive imaging equipment and radiation detection equipment;

(B) a search of the cargo; or

(C) additional information received by the Department.

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

(l) REPORT.—Not later than 270 days after the date of enactment of the Maritime Security Improvement Act of 2018, the Secretary, acting through the Commissioner, shall, in consultation with other appropriate government officials and the Commercial Operations Advisory Committee, submit a report to the appropriate congressional committees on the effectiveness of, and the need for any improvements to, the Container Security Initiative. The report shall include—

(1)<sup>2</sup> a description of the technical assistance delivered to, as well as needed at, each designated seaport;

(2) a description of the human capital management plan at each designated seaport;

(3) a summary of the requests made by the United States to foreign governments to conduct physical or non-intrusive inspections of cargo at designated seaports, and whether each such request was granted or denied by the foreign government;

(4) an assessment of the effectiveness of screening, scanning, and inspection protocols and technologies utilized at designated seaports and the effect on the flow of commerce at such seaports, as well as any recommendations for improving the effectiveness of screening, scanning, and inspection protocols and technologies utilized at designated seaports;

(5) a description and assessment of the outcome of any security incident involving a foreign seaport designated under the Container Security Initiative;

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

(7) a description of the potential for remote targeting to decrease the number of personnel who are deployed at foreign ports under CSI; and

<sup>2</sup>Margins for paragraphs (1)–(8) are so in law. Probably should be moved to the 2ems to the left.



- (8) a summary and assessment of the aggregate number and extent of trade compliance lapses at each seaport designated under the Container Security Initiative.
- (m) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the United States Customs and Border Protection to carry out the provisions of this section—
- (1) \$144,000,000 for fiscal year 2008;
  - (2) \$146,000,000 for fiscal year 2009; and
  - (3) \$153,300,000 for fiscal year 2010.

## Subtitle B—Customs-Trade Partnership Against Terrorism

### SEC. 211. [6 U.S.C. 961] ESTABLISHMENT.

(a) ESTABLISHMENT.—The Secretary, acting through the Commissioner, is authorized to establish a voluntary government-private sector 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, and to facilitate the movement of secure cargo through the international supply chain, by providing benefits to participants meeting or exceeding the program requirements. Participants in C-TPAT shall include Tier 1 participants, Tier 2 participants, and Tier 3 participants.

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

### SEC. 212. [6 U.S.C. 962] ELIGIBLE ENTITIES.

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

### SEC. 213. [6 U.S.C. 963] MINIMUM REQUIREMENTS.

An applicant seeking to participate in C-TPAT shall—

- (1) demonstrate a history of moving cargo in the international supply chain;
- (2) conduct an assessment of its supply chain based upon security criteria established by the Secretary, acting through the Commissioner, 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 established by the Commissioner; and

(4) meet all other requirements established by the Commissioner, in consultation with the Commercial Operations Advisory Committee.

**SEC. 214. [6 U.S.C. 964] TIER 1 PARTICIPANTS IN C-TPAT.**

(a) **BENEFITS.**—The Secretary, acting through the Commissioner, shall offer limited benefits to a Tier 1 participant who has been certified in accordance with the guidelines referred to in subsection (b). Such benefits may include a reduction in the score assigned pursuant to the Automated Targeting System of not greater than 20 percent of the high-risk threshold established by the Secretary.

(b) **GUIDELINES.**—Not later than 180 days after the date of the enactment of this Act, the Secretary, acting through the Commissioner, shall update the guidelines for certifying a C-TPAT participant's security measures and supply chain security practices under this section. Such guidelines shall include a background investigation and extensive documentation review.

(c) **TIMEFRAME.**—To the extent practicable, the Secretary, acting through the Commissioner, shall complete the Tier 1 certification process within 90 days of receipt of an application for participation in C-TPAT.

**SEC. 215. [6 U.S.C. 965] TIER 2 PARTICIPANTS IN C-TPAT.**

(a) **VALIDATION.**—The Secretary, acting through the Commissioner, shall validate the security measures and supply chain security practices of a Tier 1 participant in accordance with the guidelines referred to in subsection (c). Such validation shall include on-site assessments at appropriate foreign locations utilized by the Tier 1 participant in its supply chain and shall, to the extent practicable, be completed not later than 1 year after certification as a Tier 1 participant.

(b) **BENEFITS.**—The Secretary, acting through the Commissioner, shall extend benefits to each C-TPAT participant that has been validated as a Tier 2 participant under this section, which may include—

- (1) reduced scores in the Automated Targeting System;
- (2) reduced examinations of cargo; and
- (3) priority searches of cargo.

(c) **GUIDELINES.**—Not later than 180 days after the date of the enactment of this Act, the Secretary, acting through the Commissioner, shall develop a schedule and update the guidelines for validating a participant's security measures and supply chain security practices under this section.

**SEC. 216. [6 U.S.C. 966] TIER 3 PARTICIPANTS IN C-TPAT.**

(a) **IN GENERAL.**—The Secretary, acting through the Commissioner, shall establish a third tier of C-TPAT participation that offers additional benefits to participants who demonstrate a sustained commitment to maintaining security measures and supply chain security practices that exceed the guidelines established for validation as a Tier 2 participant in C-TPAT under section 215.

(b) **CRITERIA.**—The Secretary, acting through the Commissioner, shall designate criteria for validating a C-TPAT participant as a Tier 3 participant under this section. Such criteria may include—

(1) compliance with any additional guidelines established by the Secretary that exceed the guidelines established pursuant to section 215 of this Act for validating a C-TPAT participant as a Tier 2 participant, particularly with respect to controls over access to cargo throughout the supply chain;

(2) submission of additional information regarding cargo prior to loading, as determined by the Secretary;

(3) utilization of container security devices, technologies, policies, or practices that meet standards and criteria established by the Secretary; and

(4) compliance with any other cargo requirements established by the Secretary.

(c) **BENEFITS.**—The Secretary, acting through the Commissioner, in consultation with the Commercial Operations Advisory Committee and the National Maritime Security Advisory Committee, shall extend benefits to each C-TPAT participant that has been validated as a Tier 3 participant under this section, which may include—

(1) the expedited release of a Tier 3 participant's cargo in destination ports within the United States during all threat levels designated by the Secretary;

(2) further reduction in examinations of cargo;

(3) priority for examinations of cargo; and

(4) further reduction in the risk score assigned pursuant to the Automated Targeting System; and

(5) inclusion in joint incident management exercises, as appropriate.

(d) **DEADLINE.**—Not later than 2 years after the date of the enactment of this Act, the Secretary, acting through the Commissioner, shall designate appropriate criteria pursuant to subsection (b) and provide benefits to validated Tier 3 participants pursuant to subsection (c).

**SEC. 217. [6 U.S.C. 967] CONSEQUENCES FOR LACK OF COMPLIANCE.**

(a) **IN GENERAL.**—If at any time a C-TPAT participant's security measures and supply chain security practices fail to meet any of the requirements under this subtitle, the Commissioner may deny the participant benefits otherwise available under this subtitle, in whole or in part. The Commissioner shall develop procedures that provide appropriate protections to C-TPAT participants before benefits are revoked. Such procedures may not limit the ability of the Commissioner to take actions to protect the national security of the United States.

(b) **FALSE OR MISLEADING INFORMATION.**—If a C-TPAT participant knowingly provides false or misleading information to the Commissioner during the validation process provided for under this subtitle, the Commissioner shall suspend or expel the participant from C-TPAT for an appropriate period of time. The Commissioner, after the completion of the process under subsection (c), may publish in the Federal Register a list of participants who have been suspended or expelled from C-TPAT pursuant to this subsection, and may make such list available to C-TPAT participants.

(c) **RIGHT OF APPEAL.**—

(1) IN GENERAL.—A C-TPAT participant may appeal a decision of the Commissioner pursuant to subsection (a). Such appeal shall be filed with the Secretary not later than 90 days after the date of the decision, and the Secretary shall issue a determination not later than 180 days after the appeal is filed.

(2) APPEALS OF OTHER DECISIONS.—A C-TPAT participant may appeal a decision of the Commissioner pursuant to subsection (b). Such appeal shall be filed with the Secretary not later than 30 days after the date of the decision, and the Secretary shall issue a determination not later than 180 days after the appeal is filed.

**SEC. 218. [6 U.S.C. 968] THIRD PARTY VALIDATIONS.**

(a) PLAN.—The Secretary, acting through the Commissioner, shall develop a plan to implement a 1-year voluntary pilot program to test and assess the feasibility, costs, and benefits of using third party entities to conduct validations of C-TPAT participants.

(b) CONSULTATIONS.—Not later than 120 days after the date of the enactment of this Act, after consulting with private sector stakeholders, including the Commercial Operations Advisory Committee, the Secretary shall submit a report to the appropriate congressional committees on the plan described in subsection (a).

(c) PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 1 year after the consultations described in subsection (b), the Secretary shall carry out the 1-year pilot program to conduct validations of C-TPAT participants using third party entities described in subsection (a).

(2) AUTHORITY OF THE SECRETARY.—The decision to validate a C-TPAT participant is solely within the discretion of the Secretary, or the Secretary's designee.

(d) CERTIFICATION OF THIRD PARTY ENTITIES.—The Secretary shall certify a third party entity to conduct validations under subsection (c) if the entity—

(1) demonstrates to the satisfaction of the Secretary that the entity has the ability to perform validations in accordance with standard operating procedures and requirements designated by the Secretary; and

(2) agrees—

(A) to perform validations in accordance with such standard operating procedures and requirements (and updates to such procedures and requirements); and

(B) to maintain liability insurance coverage at policy limits and in accordance with conditions to be established by the Secretary; and

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

(e) INFORMATION FOR ESTABLISHING LIMITS OF LIABILITY INSURANCE.—A third party entity seeking a certificate under subsection (d) shall submit to the Secretary necessary information for establishing the limits of liability insurance required to be maintained by the entity under this Act.

(f) ADDITIONAL REQUIREMENTS.—The Secretary shall ensure that—

(1) any third party entity certified under this section does not have—

(A) any beneficial interest in or any direct or indirect control over the C-TPAT participant for which the validation services are performed; or

(B) any other conflict of interest with respect to the C-TPAT participant; and

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

(g) MONITORING.—

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

(2) REVOCATION.—If the Secretary determines that a third party entity is not meeting the minimum standard operating procedures and requirements designated by the Secretary under subsection (d)(1), the Secretary shall—

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

(B) review any validations conducted by the entity.

(h) LIMITATION ON AUTHORITY.—The Secretary may only grant a C-TPAT validation by a third party entity pursuant to subsection (c) if the C-TPAT participant voluntarily submits to validation by such third party entity.

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

(1) the results of the pilot program, including the extent to which the pilot program ensured sufficient protection for proprietary commercial information;

(2) the cost and efficiency associated with validations under the pilot program;

(3) the impact of the pilot program on the rate of validations conducted under C-TPAT;

(4) any impact on national security of the pilot program; and

(5) any recommendations by the Secretary based upon the results of the pilot program.

#### **SEC. 219. [6 U.S.C. 969] REVALIDATION.**

The Secretary, acting through the Commissioner, shall develop and implement—

(1) a revalidation process for Tier 2 and Tier 3 participants;

(2) a framework based upon objective criteria for identifying participants for periodic revalidation not less frequently than once during each 4-year period following the initial validation; and

---

**Sec. 220      Security and Accountability For Every Port Act of...      22**

---

- (3) an annual plan for revalidation that includes—
  - (A) performance measures;
  - (B) an assessment of the personnel needed to perform the revalidations; and
  - (C) the number of participants that will be revalidated during the following year.

**SEC. 220. [6 U.S.C. 970] NONCONTAINERIZED CARGO.**

The Secretary, acting through the Commissioner, shall consider the potential for participation in C-TPAT by importers of non-containerized cargoes that otherwise meet the requirements under this subtitle.

**SEC. 221. [6 U.S.C. 971] C-TPAT PROGRAM MANAGEMENT.**

(a) **IN GENERAL.**—The Secretary, acting through the Commissioner, shall establish sufficient internal quality controls and record management to support the management systems of C-TPAT. In managing the program, the Secretary shall ensure that the program includes:

(1) **STRATEGIC PLAN.**—A 5-year plan to identify outcome-based goals and performance measures of the program.

(2) **ANNUAL PLAN.**—An annual plan for each fiscal year designed to match available resources to the projected workload.

(3) **STANDARDIZED WORK PROGRAM.**—A standardized work program to be used by agency personnel to carry out the certifications, validations, and revalidations of participants. The Secretary shall keep records and monitor staff hours associated with the completion of each such review.

(b) **DOCUMENTATION OF REVIEWS.**—The Secretary, acting through the Commissioner, shall maintain a record management system to document determinations on the reviews of each C-TPAT participant, including certifications, validations, and revalidations.

(c) **CONFIDENTIAL INFORMATION SAFEGUARDS.**—In consultation with the Commercial Operations Advisory Committee, the Secretary, acting through the Commissioner, shall develop and implement procedures to ensure the protection of confidential data collected, stored, or shared with government agencies or as part of the application, certification, validation, and revalidation processes.

(d) **RESOURCE MANAGEMENT STAFFING PLAN.**—The Secretary, acting through the Commissioner, shall—

(1) develop a staffing plan to recruit and train staff (including a formalized training program) to meet the objectives identified in the strategic plan of the C-TPAT program; and

(2) provide cross-training in postincident trade resumption for personnel who administer the C-TPAT program.

(e) **REPORT TO CONGRESS.**—In connection with the President's annual budget submission for the Department, the Secretary shall report to the appropriate congressional committees on the progress made by the Commissioner to certify, validate, and revalidate C-TPAT participants. Such report shall be due on the same date that the President's budget is submitted to the Congress.

**SEC. 222. [6 U.S.C. 972] ADDITIONAL PERSONNEL.**

For fiscal years 2008 and 2009, the Commissioner shall increase by not less than 50 the number of full-time personnel engaged in the validation and revalidation of C-TPAT participants

(over the number of such personnel on the last day of the previous fiscal year), and shall provide appropriate training and support to such additional personnel.

**SEC. 223. [6 U.S.C. 973] AUTHORIZATION OF APPROPRIATIONS.**

(a) C-TPAT.—There are authorized to be appropriated to the United States Customs and Border Protection to carry out the provisions of sections 211 through 221 to remain available until expended—

- (1) \$65,000,000 for fiscal year 2008;
- (2) \$72,000,000 for fiscal year 2009; and
- (3) \$75,600,000 for fiscal year 2010.

(b) ADDITIONAL PERSONNEL.—In addition to any amounts otherwise appropriated to the United States Customs and Border Protection, there are authorized to be appropriated for the purpose of meeting the staffing requirement provided for in section 222, to remain available until expended—

- (1) \$8,500,000 for fiscal year 2008;
- (2) \$17,600,000 for fiscal year 2009;
- (3) \$19,000,000 for fiscal year 2010;
- (4) \$20,000,000 for fiscal year 2011; and
- (5) \$21,000,000 for fiscal year 2012.

## Subtitle C—Miscellaneous Provisions

**SEC. 231. [6 U.S.C. 981] PILOT INTEGRATED SCANNING SYSTEM.**

(a) DESIGNATIONS.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall designate 3 foreign seaports through which containers pass or are transshipped to the United States for the establishment of pilot integrated scanning systems that couple nonintrusive imaging equipment and radiation detection equipment. In making the designations under this subsection, the Secretary shall consider 3 distinct ports with unique features and differing levels of trade volume.

(b) COORDINATION.—The Secretary shall—

(1) coordinate with the Secretary of Energy, as necessary, to provide radiation detection equipment through the Department of Energy's Second Line of Defense and Megaports programs; or

(2) work with the private sector or, when possible, host governments to obtain radiation detection equipment that meets both the Department's and the Department of Energy's technical specifications for such equipment.

(c) PILOT SYSTEM IMPLEMENTATION.—Not later than 1 year after the date of the enactment of this Act, the Secretary shall achieve a full-scale implementation of the pilot integrated scanning system at the ports designated under subsection (a), which—

(1) shall scan all containers destined for the United States that are loaded in such ports;

(2) shall electronically transmit the images and information to appropriate United States Government personnel in the country in which the port is located or in the United States for evaluation and analysis;

(3) shall resolve every radiation alarm according to established Department procedures;

(4) shall utilize the information collected to enhance the Automated Targeting System or other relevant programs;

(5) shall store the information for later retrieval and analysis; and

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

(d) REPORT.—Not later than 180 days after achieving full-scale implementation under subsection (c), the Secretary, in consultation with the Secretary of State and, as appropriate, the Secretary of Energy, shall submit a report to the appropriate congressional committees, that includes—

(1) an evaluation of the lessons derived from the pilot system implemented under this subsection;

(2) an analysis of the efficacy of the Automated Targeting System or other relevant programs in utilizing the images captured to examine high-risk containers;

(3) an evaluation of the effectiveness of the integrated scanning system in detecting shielded and unshielded nuclear and radiological material;

(4) an evaluation of software and other technologies that are capable of automatically identifying potential anomalies in scanned containers; and

(5) an analysis of the need and feasibility of expanding the integrated scanning system to other container security initiative ports, including—

(A) an analysis of the infrastructure requirements;

(B) a projection of the effect on current average processing speed of containerized cargo;

(C) an evaluation of the scalability of the system to meet both current and future forecasted trade flows;

(D) the ability of the system to automatically maintain and catalog appropriate data for reference and analysis in the event of a transportation disruption;

(E) an analysis of requirements, including costs, to install and maintain an integrated scanning system;

(F) the ability of administering personnel to efficiently manage and utilize the data produced by a nonintrusive scanning system;

(G) the ability to safeguard commercial data generated by, or submitted to, a nonintrusive scanning system; and

(H) an assessment of the reliability of currently available technology to implement an integrated scanning system.

#### **SEC. 232. [6 U.S.C. 982] SCREENING AND SCANNING OF CARGO CONTAINERS.**

(a) ONE HUNDRED PERCENT SCREENING OF CARGO CONTAINERS AND 100 PERCENT SCANNING OF HIGH-RISK CONTAINERS.—

(1) SCREENING OF CARGO CONTAINERS.—The Secretary shall ensure that 100 percent of the cargo containers originating outside the United States and unloaded at a United



States seaport undergo a screening to identify high-risk containers.

(2) **SCANNING OF HIGH-RISK CONTAINERS.**—The Secretary shall ensure that 100 percent of the containers that have been identified as high-risk under paragraph (1), or through other means, are scanned or searched before such containers leave a United States seaport facility.

(b) **FULL-SCALE IMPLEMENTATION.**—The Secretary, in coordination with the Secretary of Energy and foreign partners, as appropriate, shall ensure integrated scanning systems are fully deployed to scan, using nonintrusive imaging equipment and radiation detection equipment, all containers entering the United States before such containers arrive in the United States as soon as possible, but not before the Secretary determines that the integrated scanning system—

- (1) meets the requirements set forth in section 231(c);
- (2) has a sufficiently low false alarm rate for use in the supply chain;
- (3) is capable of being deployed and operated at ports overseas;
- (4) is capable of integrating, as necessary, with existing systems;
- (5) does not significantly impact trade capacity and flow of cargo at foreign or United States ports; and
- (6) provides an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.

(c) **REPORT.**—Not later than 6 months after the submission of a report under section 231(d), and every 6 months thereafter, the Secretary shall submit a report to the appropriate congressional committees describing the status of full-scale deployment under subsection (b) and the cost of deploying the system at each foreign port at which the integrated scanning systems are deployed.

**SEC. 233. [6 U.S.C. 983] INSPECTION TECHNOLOGY AND TRAINING.**

(a) **IN GENERAL.**—The Secretary, in coordination with the Secretary of State, the Secretary of Energy, and appropriate representatives of other Federal agencies, may provide technical assistance, equipment, and training to facilitate the implementation of supply chain security measures at ports designated under the Container Security Initiative.

(b) **ACQUISITION AND TRAINING.**—Unless otherwise prohibited by law, the Secretary may—

- (1) lease, loan, provide, or otherwise assist in the deployment of nonintrusive inspection and radiation detection equipment at foreign land and sea ports under such terms and conditions as the Secretary prescribes, including nonreimbursable loans or the transfer of ownership of equipment; and
- (2) provide training and technical assistance for domestic or foreign personnel responsible for operating or maintaining such equipment.

**SEC. 234. FOREIGN PORT ASSESSMENTS.**

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

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

【Section 235 was repealed by section 1816(f) of division J of Public Law 115–254.】

**SEC. 236. [6 U.S.C. 985] INFORMATION SHARING RELATING TO SUPPLY CHAIN SECURITY COOPERATION.**

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

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

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

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

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

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

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

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

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

\* \* \* \* \*