CODIFICATION

Section is comprised of section 696 of Pub. L. 109–295. Subsec. (c) of section 696 of Pub. L. 109–295 amended section 5174 of Title 42, The Public Health and Welfare.

§ 796. Registry of disaster response contractors

(a) Definitions

In this section—

(1) the term ''registry'' means the registry created under subsection (b); and

(2) the terms ''small business concern'', ''small business concern owned and controlled by socially and economically disadvantaged individuals'', ''small business concern owned and controlled by women'', and ''small business concern owned and controlled by service-disabled veterans'' have the meanings given those terms under the Small Business Act (15 U.S.C. 631 et seq.).

(b) Registry

(1) In general

The Administrator shall establish and maintain a registry of contractors who are willing to perform debris removal, distribution of supplies, reconstruction, and other disaster or emergency relief activities.

(2) Contents

The registry shall include, for each business concern—

(A) the name of the business concern;

(B) the location of the business concern;

(C) the area served by the business concern;

(D) the type of good or service provided by the business concern;

(E) the bonding level of the business concern; and

(F) whether the business concern is—

(i) a small business concern;

(ii) a small business concern owned and controlled by socially and economically disadvantaged individuals;

(iii) a small business concern owned and controlled by women; or

(iv) a small business concern owned and controlled by service-disabled veterans.

(3) Source of information

(A) Submission

Information maintained in the registry shall be submitted on a voluntary basis and be kept current by the submitting business concerns.

(B) Attestation

Each business concern submitting information to the registry shall submit—

(i) an attestation that the information is true; and

(ii) documentation supporting such attestation.

(C) Verification

The Administrator shall verify that the documentation submitted by each business concern supports the information submitted by that business concern.

(4) Availability of registry

The registry shall be made generally available on the Internet site of the Agency.

(5) Consultation of registry

As part of the acquisition planning for contracting for debris removal, distribution of supplies in a disaster, reconstruction, and other disaster or emergency relief activities, a Federal agency shall consult the registry.

(Pub. L. 109–295, title VI, § 697, Oct. 4, 2006, 120 Stat. 1461.)

REFERENCES IN TEXT

The Small Business Act, referred to in subsec. (a)(2), is Pub. L. 85–536, § 2(1 et seq.), July 18, 1958, 72 Stat. 384, which is classified generally to chapter 14A (§ 631 et seq.) of Title 15, Commerce and Trade. For complete classification of this Act to the Code, see Short Title note set out under section 631 of Title 15 and Tables.

§ 797. Fraud prevention training program

The Administrator shall develop and implement a program to provide training on the prevention of waste, fraud, and abuse of Federal disaster relief assistance relating to the response to or recovery from natural disasters and acts of terrorism or other man-made disasters and ways to identify such potential waste, fraud, and abuse.

(Pub. L. 109–295, title VI, § 698, Oct. 4, 2006, 120 Stat. 1462.)

PART E—AUTHORIZATION OF APPROPRIATIONS

§ 811. Authorization of appropriations

There are authorized to be appropriated to carry out this title[1] and the amendments made by this title for the administration and operations of the Agency—

(1) for fiscal year 2008, an amount equal to the amount appropriated for fiscal year 2007 for administration and operations of the Agency, multiplied by 1.1;

(2) for fiscal year 2009, an amount equal to the amount described in paragraph (1), multiplied by 1.1; and

(3) for fiscal year 2010, an amount equal to the amount described in paragraph (2), multiplied by 1.1.

(Pub. L. 109–295, title VI, § 699, Oct. 4, 2006, 120 Stat. 1462.)

REFERENCES IN TEXT

This title, referred to in text, is title VI of Pub. L. 109–295, Oct. 4, 2006, 120 Stat. 1355, known as the Post-Katrina Emergency Management Reform Act of 2006. For complete classification of title VI to the Code, see Short Title note set out under section 701 of this title and Tables.

CHAPTER 3—SECURITY AND ACCOUNTABILITY FOR EVERY PORT

Sec.
901. Definitions.

SUBCHAPTER I—SECURITY OF UNITED STATES SEAPORTS

PART A—PORT SECURITY GRANTS; TRAINING AND EXERCISE PROGRAMS

911. Port Security Training Program.
912. Port Security Exercise Program.

[1] See References in Text note below.

Sec.
913. Facility exercise requirements.

PART B—PORT OPERATIONS

921. Domestic radiation detection and imaging.
921a. Integration of detection equipment and technologies.
922. Inspection of car ferries entering from abroad.
923. Random searches of containers.
924. Threat assessment screening of port truck drivers.
925. Border Patrol unit for United States Virgin Islands.
926. Center of Excellence for Maritime Domain Awareness.

SUBCHAPTER II—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN

PART A—GENERAL PROVISIONS

941. Strategic plan to enhance the security of the international supply chain.
942. Post-incident resumption of trade.
943. Automated Targeting System.
944. Container security standards and procedures.
945. Container Security Initiative.

PART B—CUSTOMS–TRADE PARTNERSHIP AGAINST TERRORISM

961. Establishment.
962. Eligible entities.
963. Minimum requirements.
964. Tier 1 participants in C–TPAT.
965. Tier 2 participants in C–TPAT.
966. Tier 3 participants in C–TPAT.
967. Consequences for lack of compliance.
968. Third party validations.
969. Revalidation.
970. Noncontainerized cargo.
971. C–TPAT program management.
972. Additional personnel.
973. Authorization of appropriations.

PART C—MISCELLANEOUS PROVISIONS

981. Pilot integrated scanning system.
981a. Pilot integrated scanning system.
982. Screening and scanning of cargo containers.
983. Inspection technology and training.
984. Pilot program to improve the security of empty containers.
985. Information sharing relating to supply chain security cooperation.

SUBCHAPTER III—ADMINISTRATION

1001. Designation of liaison office of Department of State.
1002. Homeland Security Science and Technology Advisory Committee.
1003. Research, development, test, and evaluation efforts in furtherance of maritime and cargo security.

§ 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).

(17) Transportation security incident

The term ''transportation security incident'' has the meaning given the term in section 70101(6) of title 46.

(Pub. L. 109–347, §2, Oct. 13, 2006, 120 Stat. 1886.)

REFERENCES IN TEXT

This Act, referred to in text, is Pub. L. 109–347, Oct. 13, 2006, 120 Stat. 1884, known as the Security and Accountability For Every Port Act of 2006 or the SAFE Port Act. For complete classification of this Act to the Code, see Tables.

Section 9503(c) of the Omnibus Budget Reconciliation Act of 1987, referred to in par. (2), is section 9503(c) of title IX of Pub. L. 100–203, which is set out as a note under section 2071 of Title 19, Customs Duties.

SHORT TITLE

Pub. L. 109–347, §1(a), Oct. 13, 2006, 120 Stat. 1884, provided that: ''This Act [see Tables for classification] may be cited as the 'Security and Accountability For Every Port Act of 2006' or the 'SAFE Port Act'.''

SUBCHAPTER I—SECURITY OF UNITED STATES SEAPORTS

PART A—PORT SECURITY GRANTS; TRAINING AND EXERCISE PROGRAMS

§911. Port Security Training Program

(a) In general

The Secretary, acting through the Under Secretary for Preparedness and in coordination with the Commandant of the Coast Guard, shall establish a Port Security Training Program (referred to in this section as the ''Training Program'') for the purpose of enhancing the capabilities of each facility required to submit a plan under section 70103(c) of title 46 to prevent, prepare for, respond to, mitigate against, and recover from threatened or actual acts of terrorism, natural disasters, and other emergencies.

(b) Requirements

The Training Program shall provide validated training that—

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

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

(3) utilizes multiple training mediums and methods;

(4) addresses port security topics, including—

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

(B) facility security force operations and management;

(C) physical security and access control at facilities;

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

(E) container security;

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

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

(H) security threats and patterns;

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

(J) evacuation procedures;

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

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

(7) addresses security requirements under facility security plans; and

(8) educates, trains, and involves individuals in neighborhoods around facilities required to submit a plan under section 70103(c) of title 46 on how to observe and report security risks.

(c) Omitted

(d) Consultation

The Secretary shall ensure that, in carrying out the Program, the Office of Grants and Training shall consult with commercial seaport personnel and management.

(e) Training partners

In developing and delivering training under the Training Program, the Secretary, in coordination with the Maritime Administration of the Department of Transportation, and consistent with section 109 of the Maritime Transportation Security Act of 2002 (46 U.S.C. 70101 note), shall—

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

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

(Pub. L. 109–347, title I, § 113, Oct. 13, 2006, 120 Stat. 1895.)

REFERENCES IN TEXT

Section 109 of the Maritime Transportation Security Act of 2002, referred to in subsec. (e), is section 109 of title I of Pub. L. 107–295, which is set out as a note under section 70101 of Title 46, Shipping.

CODIFICATION

Section is comprised of section 113 of Pub. L. 109–347. Subsec. (c) of section 113 of Pub. L. 109–347 amended section 70103 of Title 46, Shipping.

§ 912. Port Security Exercise Program

(a) In general

The Secretary, acting through the Under Secretary for Preparedness and in coordination with the Commandant of the Coast Guard, shall establish a Port Security Exercise Program (referred to in this section as the ''Exercise Program'') for the purpose of testing and evaluating the capabilities of Federal, State, local, and foreign governments, commercial seaport personnel and management, governmental and nongovernmental emergency response providers, the private sector, or any other organization or entity, as the Secretary determines to be appropriate, to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism, natural disasters, and other emergencies at facilities required to submit a plan under section 70103(c) of title 46.

(b) Requirements

The Secretary shall ensure that the Exercise Program—

(1) conducts, on a periodic basis, port security exercises at such facilities that are—

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

(B) live, in the case of the most at-risk facilities;

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

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

(E) evaluated against clear and consistent performance measures;

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

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

(2) assists State and local governments and facilities in designing, implementing, and evaluating exercises that—

(A) conform to the requirements of paragraph (1); and

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

(c) Improvement plan

The Secretary shall establish a port security exercise improvement plan process to—

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

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

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

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

(Pub. L. 109–347, title I, § 114, Oct. 13, 2006, 120 Stat. 1896.)

§ 913. Facility exercise requirements

The Secretary of the Department in which the Coast Guard is operating shall require each high risk facility to conduct live or full-scale exercises described in section 105.220(c) of title 33, Code of Federal Regulations, not less frequently than once every 2 years, in accordance with the facility security plan required under section 70103(c) of title 46.

(Pub. L. 109–347, title I, § 115, Oct. 13, 2006, 120 Stat. 1897.)

PART B—PORT OPERATIONS

§ 921. Domestic radiation detection and imaging

(a) Scanning containers

Subject to section 1318 of title 19, 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) Report

Not later than 90 days after October 13, 2006, the Secretary shall submit the strategy developed under subsection (b) to the appropriate congressional committees.

(d) Update

Not later than 180 days after the date of the submission of the report under subsection (c), the Secretary shall provide a more complete evaluation under subsection (b)(6).

(e) Other weapons of mass destruction threats

Not later than 180 days after October 13, 2006, the Secretary shall submit to the appropriate congressional committees a report on the feasibility of, and a strategy for, the development of equipment to detect and prevent shielded nuclear and radiological threat material and chemical, biological, and other weapons of mass destruction from entering the United States.

(f) 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.

(g) Implementation

Not later than 3 years after October 13, 2006, the Secretary shall fully implement the strategy developed under subsection (b).

(h) 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) (and updating, if any, of that strategy under subsection (c)),

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.

(i) 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.

(Pub. L. 109–347, title I, § 121, Oct. 13, 2006, 120 Stat. 1898.)

§ 921a. Integration of detection equipment and technologies

(a) Responsibility of Secretary

The Secretary of Homeland Security shall have responsibility for ensuring that domestic chemical, biological, radiological, and nuclear detection equipment and technologies are integrated, as appropriate, with other border security systems and detection technologies.

(b) Report

Not later than 6 months after August 3, 2007, the Secretary shall submit a report to Congress that contains a plan to develop a departmental technology assessment process to determine and

certify the technology readiness levels of chemical, biological, radiological, and nuclear detection technologies before the full deployment of such technologies within the United States.

(Pub. L. 110–53, title XI, §1104, Aug. 3, 2007, 121 Stat. 380.)

CODIFICATION

Section was enacted as part of the Implementing Recommendations of the 9/11 Commission Act of 2007, and not as part of the Security and Accountability For Every Port Act of 2006, also known as the SAFE Port Act, which comprises this chapter.

§ 922. Inspection of car ferries entering from abroad

Not later than 120 days after October 13, 2006, the Secretary, acting through the Commissioner, and in coordination with the Secretary of State and in cooperation with ferry operators and appropriate foreign government officials, shall seek to develop a plan for the inspection of passengers and vehicles before such passengers board, or such vehicles are loaded onto, a ferry bound for a United States facility required to submit a plan under section 70103(c) of title 46.

(Pub. L. 109–347, title I, §122, Oct. 13, 2006, 120 Stat. 1899.)

§ 923. Random searches of containers

Not later than 1 year after October 13, 2006, the Secretary, acting through the Commissioner, shall develop and implement a plan, utilizing best practices for empirical scientific research design and random sampling, to conduct random searches of containers in addition to any targeted or preshipment inspection of such containers required by law or regulation or conducted under any other program conducted by the Secretary. Nothing in this section shall be construed to mean that implementation of the random sampling plan precludes additional searches of containers not inspected pursuant to the plan.

(Pub. L. 109–347, title I, §123, Oct. 13, 2006, 120 Stat. 1899.)

§ 924. Threat assessment screening of port truck drivers

Not later than 90 days after October 13, 2006, the Secretary shall implement a threat assessment screening, including name-based checks against terrorist watch lists and immigration status check, for all port truck drivers with access to secure areas of a port who have a commercial driver's license but do not have a current and valid hazardous materials endorsement issued in accordance with section 1572 of title 49, Code of Federal Regulations, that is the same as the threat assessment screening required for facility employees and longshoremen by the Commandant of the Coast Guard under Coast Guard Notice USCG–2006–24189 (Federal Register, Vol. 71, No. 82, Friday, April 28, 2006).

(Pub. L. 109–347, title I, §125, Oct. 13, 2006, 120 Stat. 1900.)

§ 925. Border Patrol unit for United States Virgin Islands

(a) In general

The Secretary may establish at least 1 Border Patrol unit for the United States Virgin Islands.

(b) Report

Not later than 180 days after October 13, 2006, the Secretary shall submit a report to the appropriate congressional committees that includes the schedule, if any, for carrying out subsection (a).

(Pub. L. 109–347, title I, §126, Oct. 13, 2006, 120 Stat. 1900.)

§ 926. Center of Excellence for Maritime Domain Awareness

(a) Establishment

The Secretary shall establish a university-based Center for Excellence for Maritime Domain Awareness following the merit-review processes and procedures that have been established by the Secretary for selecting university program centers of excellence.

(b) Duties

The Center established under subsection (a) shall—

(1) prioritize its activities based on the ''National Plan To Improve Maritime Domain Awareness'' published by the Department in October 2005;

(2) recognize the extensive previous and ongoing work and existing competence in the field of maritime domain awareness at numerous academic and research institutions, such as the Naval Postgraduate School;

(3) leverage existing knowledge and continue development of a broad base of expertise within academia and industry in maritime domain awareness; and

(4) provide educational, technical, and analytical assistance to Federal agencies with responsibilities for maritime domain awareness, including the Coast Guard, to focus on the need for interoperability, information sharing, and common information technology standards and architecture.

(Pub. L. 109–347, title I, §128, Oct. 13, 2006, 120 Stat. 1900.)

SUBCHAPTER II—SECURITY OF THE INTERNATIONAL SUPPLY CHAIN

PART A—GENERAL PROVISIONS

§ 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, as appropriate, a strategic plan to enhance the security of the international supply chain.

(b) Requirements

The strategic plan required under subsection (a) shall—

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

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

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

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

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

(6) provide incentives for additional voluntary measures to enhance cargo security, as 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 942 of this title;

(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) Report

(1) Initial report

Not later than 270 days after October 13, 2006, 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 3 years after the date on which the strategic plan is submitted under paragraph (1), the Secretary shall submit a report to the appropriate congressional committees that contains an update of the strategic plan.

(Pub. L. 109–347, title II, §201, Oct. 13, 2006, 120 Stat. 1901.)

§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 941(b)(10) of this title 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), 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 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; 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 941 of this title, 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.

(Pub. L. 109–347, title II, § 202, Oct. 13, 2006, 120 Stat. 1903.)

§ 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.

(Pub. L. 109–347, title II, §203, Oct. 13, 2006, 120 Stat. 1904.)

REFERENCES IN TEXT

Section 343(a) of the Trade Act of 2002, referred to in subsec. (d), is section 343(a) of title III of div. A of Pub. L. 107–210, which is set out as a note under section 2071 of Title 19, Customs Duties.

§944. Container security standards and procedures

(a) Establishment

(1) In general

Not later than 90 days after October 13, 2006, the Secretary shall initiate a rulemaking 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 October 13, 2006, 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 international trade obligations or other international obligations of the United States.

(Pub. L. 109–347, title II, §204, Oct. 13, 2006, 120 Stat. 1905; Pub. L. 110–53, title XVII, §1701(b), Aug. 3, 2007, 121 Stat. 491.)

AMENDMENTS

2007—Subsec. (a)(4). Pub. L. 110–53, which directed amendment of par. (4) by substituting ''(1) Deadline for enforcement'' and subpar. (A) designation and heading for ''(1) Deadline for enforcement'', was executed by inserting the subpar. (A) designation and heading before ''Not later than'' and making no change in the par. designation or heading, to reflect the probable intent of Congress.

Subsec. (a)(4)(B). Pub. L. 110–53, §1701(b)(2), added subpar. (B).

§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 par-

ticipate 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;

(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 des-

ignated 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

(1) In general

Not later than September 30, 2007, 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—

(A) a description of the technical assistance delivered to, as well as needed at, each designated seaport;

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

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

(D) 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;

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

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

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

(H) a summary and assessment of the aggregate number and extent of trade compliance lapses at each seaport designated under the Container Security Initiative.

(2) Updated report

Not later than September 30, 2010, the Secretary, acting through the Commissioner, shall, in consultation with other appropriate government officials and the Commercial Operations Advisory Committee, submit an updated report to the appropriate congressional committees on the effectiveness of, and the need for any improvements to, the Container Security Initiative. The updated report shall address each of the elements required to be included in the report provided for under paragraph (1).

(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.

(Pub. L. 109–347, title II, § 205, Oct. 13, 2006, 120 Stat. 1906.)

PART B—CUSTOMS–TRADE PARTNERSHIP AGAINST TERRORISM

§ 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.

(Pub. L. 109–347, title II, § 211, Oct. 13, 2006, 120 Stat. 1909.)

§ 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.

(Pub. L. 109–347, title II, § 212, Oct. 13, 2006, 120 Stat. 1909.)

§ 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.

(Pub. L. 109–347, title II, § 213, Oct. 13, 2006, 120 Stat. 1909.)

§ 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 October 13, 2006, 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.

(Pub. L. 109–347, title II, § 214, Oct. 13, 2006, 120 Stat. 1910.)

§ 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 October 13, 2006, 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.

(Pub. L. 109–347, title II, § 215, Oct. 13, 2006, 120 Stat. 1910.)

§ 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 965 of this title.

(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 965 of this title 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 October 13, 2006, 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).

(Pub. L. 109–347, title II, § 216, Oct. 13, 2006, 120 Stat. 1910.)

§ 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 part, the Commissioner may deny the participant benefits otherwise available under this part, 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 part, 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.

(Pub. L. 109–347, title II, § 217, Oct. 13, 2006, 120 Stat. 1911.)

§ 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 October 13, 2006, 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 require-

ments 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.

(Pub. L. 109–347, title II, § 218, Oct. 13, 2006, 120 Stat. 1912.)

REFERENCES IN TEXT

This Act, referred to in subsec. (e), is Pub. L. 109–347, Oct. 13, 2006, 120 Stat. 1884, known as the Security and Accountability For Every Port Act of 2006 or the SAFE Port Act. For complete classification of this Act to the Code, see Tables.

§ 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

(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.

(Pub. L. 109–347, title II, § 219, Oct. 13, 2006, 120 Stat. 1913.)

§ 970. Noncontainerized cargo

The Secretary, acting through the Commissioner, shall consider the potential for participation in C–TPAT by importers of noncontainerized cargoes that otherwise meet the requirements under this part.

(Pub. L. 109–347, title II, § 220, Oct. 13, 2006, 120 Stat. 1914.)

§ 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.

(Pub. L. 109–347, title II, § 221, Oct. 13, 2006, 120 Stat. 1914.)

§ 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.

(Pub. L. 109–347, title II, § 222, Oct. 13, 2006, 120 Stat. 1914.)

§ 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 961 through 971 of this title 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 972 of this title, 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.

(Pub. L. 109–347, title II, § 223, Oct. 13, 2006, 120 Stat. 1915.)

PART C—MISCELLANEOUS PROVISIONS

§ 981. Pilot integrated scanning system

(a) Designations

Not later than 90 days after October 13, 2006, 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 October 13, 2006, 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.

(Pub. L. 109–347, title II, § 231, Oct. 13, 2006, 120 Stat. 1915.)

§ 981a. Pilot integrated scanning system

(a) Designations

(1) In general

Not later than 90 days after October 4, 2006, the Secretary of Homeland Security (referred to in this section as the ''Secretary'') shall designate three foreign seaports through which containers pass or are transshipped to the United States to pilot an integrated scanning system that couples nonintrusive imaging equipment and radiation detection equipment, which may be provided by the Megaports Initiative of the Department of Energy. In making designations under this subsection, the Secretary shall consider three distinct ports with unique features and differing levels of trade volume.

(2) Collaboration and cooperation

The Secretary shall collaborate with the Secretary of Energy and cooperate with the private sector and host foreign government to implement the pilot program under this subsection.

(b) Implementation

Not later than one year after October 4, 2006, the Secretary shall achieve a full-scale implementation of the pilot integrated screening system, which shall—

(1) scan all containers destined for the United States that transit through the terminal;

(2) electronically transmit the images and information to the container security initiative personnel in the host country and/or Customs and Border Protection personnel in the United States for evaluation and analysis;

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

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

(5) store the information for later retrieval and analysis.

(c) Evaluation

The Secretary shall evaluate the pilot program in subsection (b) to determine whether such a system—

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

(2) is capable of being deployed and operated at ports overseas, including consideration of cost, personnel, and infrastructure required to operate the system;

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

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

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

(d) Report

Not later than 120 days after achieving full-scale implementation under subsection (b), the Secretary, in consultation with the Secretary of Energy and the Secretary of State, shall submit a report, to the appropriate congressional committees, that includes—

(1) an evaluation of the lessons derived from the pilot program implemented under this section;

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

(3) an evaluation of software that is capable of automatically identifying potential anomalies in scanned containers; and

(4) a plan and schedule to expand the integrated scanning system developed under this section to other container security initiative ports.

(e) Implementation

If the Secretary determines the available technology meets the criteria outlined in subsection (c), the Secretary, in cooperation with the Secretary of State, shall seek to secure the cooperation of foreign governments to initiate and maximize the use of such technology at foreign ports to scan all cargo bound for the United States as quickly as possible.

(Pub. L. 109–295, title V, § 558, Oct. 4, 2006, 120 Stat. 1392.)

CODIFICATION

Section was enacted as part of the Department of Homeland Security Appropriations Act, 2007, and not as part of the Security and Accountability For Every Port Act of 2006, also known as the SAFE Port Act, which comprises this chapter.

§ 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

(1) In general

A container that was loaded on a vessel in a foreign port shall not enter the United States (either directly or via a foreign port) unless the container was scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel.

(2) Application

Paragraph (1) shall apply with respect to containers loaded on a vessel in a foreign country on or after the earlier of—

(A) July 1, 2012; or

(B) such other date as may be established by the Secretary under paragraph (3).

(3) Establishment of earlier deadline

The Secretary shall establish a date under (2)(B)[1] pursuant to the lessons learned through the pilot integrated scanning systems established under section 981 of this title.

(4) Extensions

The Secretary may extend the date specified in paragraph (2)(A) or (2)(B) for 2 years, and may renew the extension in additional 2-year increments, for containers loaded in a port or ports, if the Secretary certifies to Congress that at least two of the following conditions exist:

(A) Systems to scan containers in accordance with paragraph (1) are not available for purchase and installation.

(B) Systems to scan containers in accordance with paragraph (1) do not have a sufficiently low false alarm rate for use in the supply chain.

(C) Systems to scan containers in accordance with paragraph (1) cannot be purchased, deployed, or operated at ports overseas, including, if applicable, because a port does not have the physical characteristics to install such a system.

(D) Systems to scan containers in accordance with paragraph (1) cannot be integrated, as necessary, with existing systems.

(E) Use of systems that are available to scan containers in accordance with paragraph (1) will significantly impact trade capacity and the flow of cargo.

(F) Systems to scan containers in accordance with paragraph (1) do not adequately provide an automated notification of questionable or high-risk cargo as a trigger for further inspection by appropriately trained personnel.

(5) Exemption for military cargo

Notwithstanding any other provision in the section, supplies bought by the Secretary of Defense and transported in compliance section 2631 of title 10 and military cargo of foreign countries are exempt from the requirements of this section.

(6) Report on extensions

An extension under paragraph (4) for a port or ports shall take effect upon the expiration of the 60-day period beginning on the date the Secretary provides a report to Congress that—

(A) states what container traffic will be affected by the extension;

(B) provides supporting evidence to support the Secretary's certification of the basis for the extension; and

(C) explains what measures the Secretary is taking to ensure that scanning can be implemented as early as possible at the port or ports that are the subject of the report.

(7) Report on renewal of extension

If an extension under paragraph (4) takes effect, the Secretary shall, after one year, submit a report to Congress on whether the Secretary expects to seek to renew the extension.

[1] So in original. Probably should be ''paragraph (2)(B)''.

(8) Scanning technology standards

In implementing paragraph (1), the Secretary shall—

(A) establish technological and operational standards for systems to scan containers;

(B) ensure that the standards are consistent with the global nuclear detection architecture developed under the Homeland Security Act of 2002 [6 U.S.C. 101 et seq.]; and

(C) coordinate with other Federal agencies that administer scanning or detection programs at foreign ports.

(9) International trade and other obligations

In carrying out this subsection, the Secretary shall consult with appropriate Federal departments and agencies and private sector stakeholders, and ensure that actions under this section do not violate international trade obligations, and are consistent with the World Customs Organization framework, or other international obligations of the United States.

(c) Report

Not later than 6 months after the submission of a report under section 981(d) of this title, 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.

(Pub. L. 109–347, title II, § 232, Oct. 13, 2006, 120 Stat. 1916; Pub. L. 110–53, title XVII, § 1701(a), Aug. 3, 2007, 121 Stat. 489.)

REFERENCES IN TEXT

The Homeland Security Act of 2002, referred to in subsec. (b)(8)(B), is Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, which is classified principally to chapter 1 (§ 101 et seq.) of this title. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

AMENDMENTS

2007—Subsec. (b). Pub. L. 110–53 reenacted heading without change and amended text of subsec. (b) generally. Prior to amendment, text related to full deployment of an integrated scanning system after the Secretary had determined that such system had met section 981(c) requirements, had a sufficiently low false alarm rate, was capable of being deployed overseas, was capable of integrating with existing systems, would not significantly impact trade flow, and had provided for automated notification of high-risk cargo.

§ 983. Inspection technology and training

(1) 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.

(2) Acquisition and training

Unless otherwise prohibited by law, the Secretary may—

(A) 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

(B) provide training and technical assistance for domestic or foreign personnel responsible for operating or maintaining such equipment.

(Pub. L. 109–347, title II, § 233(a), Oct. 13, 2006, 120 Stat. 1917.)

§ 984. Pilot program to improve the security of empty containers

(a) In general

The Secretary shall conduct a 1-year pilot program to assess the risk posed by and improve the security of empty containers at United States seaports to ensure the safe and secure delivery of cargo and to prevent potential acts of terrorism involving such containers. The pilot program shall include the use of visual searches of empty containers at United States seaports.

(b) Report

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

(1) the results of the pilot program; and

(2) the determination of the Secretary on whether to expand the pilot program.

(Pub. L. 109–347, title II, § 235, Oct. 13, 2006, 120 Stat. 1919.)

§ 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.

(Pub. L. 109–347, title II, § 236, Oct. 13, 2006, 120 Stat. 1919.)

SUBCHAPTER III—ADMINISTRATION

§ 1001. Designation of liaison office of Department of State

The Secretary of State shall designate a liaison office within the Department of State to assist the Secretary, as appropriate, in negotiating cargo security-related international agreements.

(Pub. L. 109–347, title III, § 301(b), Oct. 13, 2006, 120 Stat. 1920.)

RULE OF CONSTRUCTION

Nothing in this section to be construed to affect the authorities, functions, or capabilities of the Coast Guard to perform its missions or the requirement under section 468 of this title that those authorities, functions, and capabilities be maintained intact, see section 301(c) of Pub. L. 109–347, set out as a note under section 239 of this title.

§ 1002. Homeland Security Science and Technology Advisory Committee

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

(Pub. L. 109–347, title III, § 302(c), Oct. 13, 2006, 120 Stat. 1921.)

§ 1003. Research, development, test, and evaluation efforts in furtherance of maritime and cargo security

(a) In general

The Secretary shall—

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

(2) coordinate with public and private sector entities to develop and test technologies, and process innovations in furtherance of these objectives; and

(3) evaluate such technologies.

(b) Coordination

The Secretary, in coordination with the Under Secretary for Science and Technology, the As-

sistant Secretary for Policy, the Commandant of the Coast Guard, the Director for Domestic Nuclear Detection, the Chief Financial Officer, and the heads of other appropriate offices or entities of the Department, shall ensure that—

(1) research, development, testing, and evaluation efforts funded by the Department in furtherance of maritime and cargo security are coordinated within the Department and with other appropriate Federal agencies to avoid duplication of efforts; and

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

(Pub. L. 109–347, title III, § 303, Oct. 13, 2006, 120 Stat. 1921.)

CHAPTER 4—TRANSPORTATION SECURITY

SUBCHAPTER I—TRANSPORTATION SECURITY PLANNING AND INFORMATION SHARING

Sec.
1101. Definitions.
1102. National Domestic Preparedness Consortium.
1103. National Transportation Security Center of Excellence.
1104. Immunity for reports of suspected terrorist activity or suspicious behavior and response.

SUBCHAPTER II—TRANSPORTATION SECURITY ENHANCEMENTS

1111. Definitions.
1112. Authorization of Visible Intermodal Prevention and Response teams.
1113. Surface transportation security inspectors.
1114. Surface transportation security technology information sharing.
1115. TSA personnel limitations.
1116. National explosives detection canine team training program.
1117. Roles of the Department of Homeland Security and the Department of Transportation.

SUBCHAPTER III—PUBLIC TRANSPORTATION SECURITY

1131. Definitions.
1132. Findings.
1133. National Strategy for Public Transportation Security.
1134. Security assessments and plans.
1135. Public transportation security assistance.
1136. Security exercises.
1137. Public transportation security training program.
1138. Public transportation research and development.
1139. Information sharing.
1140. Threat assessments.
1141. Reporting requirements.
1142. Public transportation employee protections.
1143. Security background checks of covered individuals for public transportation.
1144. Limitation on fines and civil penalties.

SUBCHAPTER IV—SURFACE TRANSPORTATION SECURITY

PART A—GENERAL PROVISIONS

1151. Definitions.
1152. Oversight and grant procedures.
1153. Authorization of appropriations.
1154. Public awareness.

PART B—RAILROAD SECURITY

1161. Railroad transportation security risk assessment and National Strategy.
Sec.
1162. Railroad carrier assessments and plans.
1163. Railroad security assistance.
1164. Systemwide Amtrak security upgrades.
1165. Fire and life safety improvements.
1166. Railroad carrier exercises.
1167. Railroad security training program.
1168. Railroad security research and development.
1169. Railroad tank car security testing.
1170. Security background checks of covered individuals.
1171. International railroad security program.
1172. Railroad security enhancements; Model State legislation.

PART C—OVER-THE-ROAD BUS AND TRUCKING SECURITY

1181. Over-the-road bus security assessments and plans.
1182. Over-the-road bus security assistance.
1183. Over-the-road bus exercises.
1184. Over-the-road bus security training program.
1185. Over-the-road bus security research and development.
1186. Memorandum of Understanding annex.

PART D—HAZARDOUS MATERIAL AND PIPELINE SECURITY

1201. Railroad routing of security-sensitive materials.
1202. Railroad security-sensitive material tracking.
1203. Hazardous materials highway routing.
1204. Motor carrier security-sensitive material tracking.
1205. Hazardous materials security inspections and study.
1206. Use of transportation security card in hazmat licensing.
1207. Pipeline security inspections and enforcement.
1208. Pipeline security and incident recovery plan.

SUBCHAPTER I—TRANSPORTATION SECURITY PLANNING AND INFORMATION SHARING

§ 1101. Definitions

For purposes of this subchapter, the following terms apply:

(1) Department

The term ''Department'' means the Department of Homeland Security.

(2) Secretary

The term ''Secretary'' means the Secretary of Homeland Security.

(Pub. L. 110–53, title XII, § 1201, Aug. 3, 2007, 121 Stat. 381.)

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original ''this title'', meaning title XII of Pub. L. 110–53, Aug. 3, 2007, 121 Stat. 381, which enacted this subchapter, amended section 114 of Title 49, Transportation, and enacted provisions set out as a note under section 114 of Title 49. For complete classification of title XII to the Code, see Tables.

SHORT TITLE

Pub. L. 110–53, title XIV, § 1401, Aug. 3, 2007, 121 Stat. 400, provided that: ''This title [enacting subchapter III of this chapter] may be cited as the 'National Transit Systems Security Act of 2007'.''

EX. ORD. NO. 13416. STRENGTHENING SURFACE TRANSPORTATION SECURITY

Ex. Ord. No. 13416, Dec. 5, 2006, 71 F.R. 71033, provided: