S. HRG. 110–1185

THE SECURITY OF OUR NATION'S PORTS

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

OCTOBER 4, 2007

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

77–233 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

DANIEL K. INOUYE, Hawaii, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska, *Vice Chairman*
JOHN F. KERRY, Massachusetts	JOHN MCCAIN, Arizona
BYRON L. DORGAN, North Dakota	TRENT LOTT, Mississippi
BARBARA BOXER, California	KAY BAILEY HUTCHISON, Texas
BILL NELSON, Florida	OLYMPIA J. SNOWE, Maine
MARIA CANTWELL, Washington	GORDON H. SMITH, Oregon
FRANK R. LAUTENBERG, New Jersey	JOHN ENSIGN, Nevada
MARK PRYOR, Arkansas	JOHN E. SUNUNU, New Hampshire
THOMAS R. CARPER, Delaware	JIM DEMINT, South Carolina
CLAIRE MCCASKILL, Missouri	DAVID VITTER, Louisiana
AMY KLOBUCHAR, Minnesota	JOHN THUNE, South Dakota

MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
LILA HARPER HELMS, *Democratic Deputy Staff Director and Policy Director*
CHRISTINE D. KURTH, *Republican Staff Director and General Counsel*
PAUL NAGLE, *Republican Chief Counsel*

CONTENTS

THE SECURITY OF OUR NATION'S PORTS

THURSDAY, OCTOBER 4, 2007

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m., in room SR–253, Russell Senate Office Building, Hon. Frank R. Lautenberg, presiding.

OPENING STATEMENT OF HON. FRANK R. LAUTENBERG, U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. Good morning. Oh, the junior member of the twosome here is a little late arriving. I just got up and something reminded me that being on time is critical. I can't blame it on traffic because it would only have been foot traffic. But we welcome all of you here. Thank you very much for being here.

Today's hearing is going to be on the security of our ports and their impact on the safety of our country. Our ports serve as a doorway to America. The New Jersey/New York port is the second biggest container port in the country and it lies along a two-mile stretch. It has been identified by the FBI as the two most dangerous miles in the country for a terrorist attack. It's the area between Newark Liberty Airport and the Port of New York and New Jersey. Thousands of people work there and 12 million others, residents and commuters, are present in the nearby communities, 12 million people.

So I'm particularly pleased to have the person who oversees this port, Chairman Tony Coscia, someone I know very well while I was a member of the Port Authority Board, for several years. That experience helped guide me into the portfolio that I focus so actively on; that is, transportation.

One year ago, Congress passed a comprehensive port security bill and the GAO recently declared that maritime security is one of the few areas where the Department of Homeland Security has improved. For instance, Port Security Grants are awarded almost exclusively on risk and I've worked hard to get all of our security grants based on risk. And after years of under-funding, the Port Security Grant Program is starting to get the money that it needs, $320 million in Fiscal Year 2007 and we're working to get even more necessary funding in 2008, even though the Department of Homeland Security appropriations bill is operating under a veto threat.

But even with this progress, there are still holes that riddle our port security network. We held our last hearing on the Transpor-

tation Worker Identification Credential (TWIC) Program six months ago and it's almost incomprehensible to report that the program and worker security is stuck in neutral. Six years after 9/11 and nearly $100 million later, only 1,700 workers have working TWIC cards and that's with more than a million and a half people working in the port areas. That cost, by the way, is nearly $60,000 a card and we still don't even have a deployment schedule for when the rest of the cards will get into workers' hands.

Also, the SAFE Port Act calls for a system to scan every U.S.-bound shipping container for deadly weapons before they arrive on our shores. These containers, obviously, can carry anything imaginable—nuclear, radiological, chemical or biological weapons. Today, they have a 95 percent chance of not being physically inspected and that's why we need to be scanning these containers.

Now, I'm anxious to hear what progress the Bush Administration has made toward achieving 100 percent scanning of the containers. Until we get there, the U.S. Customs and Border Protection's automated targeting system is our front line against cargo security risks. If the data we use to target shipments is not reliable, robust or valid, the system fails and the risk for the American people increases. I want to know when Customs will upgrade this system to track suspicious shipments with more accuracy by requiring additional data on each shipment.

Finally, securing our seaports will take greater investment to prevent a tragedy potentially even larger than the deadly and devastating attack that took place on 9/11. The Port of New York and New Jersey has suggested that Congress collect a security fee on each container entering the United States to provide this greater funding. So I look forward to hearing from today's witnesses on their suggestions as well as their views on our overall port security and now I would call on Senator Stevens for his statement.

STATEMENT OF HON. TED STEVENS,
U.S. SENATOR FROM ALASKA

Senator STEVENS. Thank you, Mr. Chairman. I'll be brief. It's almost a month ago that we marked the sixth year since 9/11, and we continue to face monumental challenges in securing our ports and the territorial waters and the total transportation system. Maritime commerce is the lifeblood of international trade and we are the world's leading maritime trading nation. And Mr. Chairman, let me put my whole statement in the record, if I may.

I'll just briefly summarize it. As far as I'm concerned, we live in an area that is totally dependent upon this industry and there's no question that at our port, about 90 percent of the goods that we depend on come in through the Port of Anchorage. And now we have a dream that we'll be able to extend the Alaska Railroad up to the Canadian border and tie into the Canadian National Railway System and be able to bring the products of the Pacific to the people in northwestern Canada.

I do believe that the whole concept of security is the important concept we have to work on. I think we should continue to improve our security plans, our interagency cooperation, the methods of implementing the Transportation Workers Identification Credential system and the other innovative technologies that will provide us

greater security for our ports. So I look forward to hearing your statements today and Mr. Chairman, I thank you very much for the privilege of making my comments.

[The prepared statement of Senator Stevens follows:]

PREPARED STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

Almost 1 month ago we marked 6 years since 9/11 and as a Nation we continue to face the monumental challenges in securing our ports, territorial waters and transportation systems.

Maritime commerce is the lifeblood of international trade, and the United States is the world's leading maritime trading nation. The U.S. maritime transportation system contributes more than $740 billion to our gross domestic product and employs more than 13 million citizens.

Alaskans have long since realized our economy is dependent on our seaports. Ninety percent of Alaska's consumer goods travel through the port of Anchorage. Additionally thousands of ships transit Alaska's waters to and from Asia along the great circle route. It is essential that we have the ability to track these ships.

We must remain steadfast in our resolve to protect the Nation's seaports and supply chains. I recognize the progress made by the U.S. Coast Guard, Customs and Border Protection, and the Transportation Security Administration over the last several years.

But we have much more work to do. We must continue to focus on honing our security plans, improving interagency cooperation, implementing the Transportation Workers Identification Card system, and using the most innovative technologies to secure our supply chains.

I welcome our witnesses, and look forward to hearing from them on how we can continue to strengthen our maritime security systems.

Senator LAUTENBERG. Thank you, Senator Stevens. Keeping with party to party, I call on Senator Cantwell.

STATEMENT OF HON. MARIA CANTWELL, U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Mr. Chairman and thank you for holding this important hearing. Our Nation's ports are an integral part of the fabric of our Nation's economy and certainly now, improvement in its security is of utmost importance. The U.S. ports handle more than 95 percent of our national overseas trade and the total volume of goods shipped from the U.S. is expected to double over the next 20 years. So ensuring security and safety of our ports, as I said, is of utmost importance.

We know this well in Washington State because Puget Sound is one of the most busy and complex waterways in the world. The ports of Seattle and Tacoma are the Nation's third largest port center and move more than 11,000 cargo containers daily. Cruise ship traffic has increased tenfold in 8 years, from five vessel calls in 1990 to 200 vessel calls last year and oil tankers and tank barges made more than 4,000 trips across Puget Sound last year and our ferry system covers more than 25 million passengers each year. That's more than the Amtrak system. So let's just say we have a very busy waterway in the Northwest. We're also home to a lot of other smaller ports but very important ports in Washington State that carry everything from our agriculture products to various markets in Asia overseas and we certainly have quite a few pleasure boats traffic coming between U.S. and Canadian waters that also demand Custom's import inspection.

All of these activities make the security of our waterway system one of our most complex challenges and we depend on the Coast

Guard and Border Protection to make sure that security is implemented. Our laws, such as the Marine Transportation Security Act and SAFE Port Act have established a strong framework for improving our national port security but these important programs and their implementation are challenging us, I believe, to look further beyond—to get that system deployment done and done effectively, but also to look beyond our U.S. shores to make sure that the implementation of these overseas inspections are also happening. I firmly believe that waiting until cargo gets to the United States is a little late and making sure that we actually have the resources, so Admiral Pekoske, I plan on asking you about whether we have sufficient funds to do those international inspections that are so important for our port security.

Since 9/11, the Coast Guard's maritime and security mission has grown significantly, making sure that we have the resources to carry out that and also making sure that the acquisition of those resources are done in an effective manner that doesn't delay but delivers and is done cost effectively for the taxpayers is something that we are going to continue to explore. So I look forward to hearing the testimony, Mr. Chairman and again, thank you for this important hearing.

Senator LAUTENBERG. Thank you, Senator Cantwell. Senator Smith?

STATEMENT OF HON. GORDON H. SMITH,
U.S. SENATOR FROM OREGON

Senator SMITH. Thank you, Mr. Chairman. I thank you for this hearing and I thank our witnesses. I'm anxious to hear them because like Senator Cantwell, trade is absolutely central to my state's economy and our ports are connections to other markets around the world. The secure and efficient movement of goods is absolutely critical to maintaining a vibrant economy in my state and in the Northwest and around the country. So as we approach the 1-year anniversary of the enactment of the SAFE Port Act, I'm anxious to learn how we can make it even better. Thank you.

Senator LAUTENBERG. Thanks very much, Senator Smith. And now, in the order of the seating, Rear Admiral David Pekoske, we welcome you, Admiral, as Assistant Commandant for Operations for the Coast Guard and after Rear Admiral Pekoske, we'll hear from Ms. Fanguy, the TWIC Program Director for Transportation Security Administration and as you can imagine, Ms. Fanguy, we'll have a few questions and the Honorable Thomas Winkowski, Assistant Commissioner of Field Operations for the United States Customs and Border Protection. Mr. Stephen Caldwell, the Director for Homeland Security and Justice Issues for GAO and finally, a friend and colleague from New Jersey, Mr. Anthony Coscia, once again, Chairman of the Board of the Commissioners of the—I'll call it the Regional Port Authority because we always have a problem about which comes first, whether it's New York or New Jersey Port Authority but it's a wonderful agency and Mr. Coscia, we're pleased to have you here with us. You all have a lot of responsibility overseeing the largest port on the East Coast and we appreciate the perspective you provide. Thank you all again for being here. We

have a 5 minute time limit for your presentation and once again, Admiral Pekoske, welcome.

STATEMENT OF REAR ADMIRAL DAVID P. PEKOSKE, ASSISTANT COMMANDANT FOR OPERATIONS, U.S. COAST GUARD, DEPARTMENT OF HOMELAND SECURITY

Admiral PEKOSKE. Thank you, Mr. Chairman. Good morning, Mr. Chairman and Mr. Vice-Chairman and distinguished Members of the Committee. It is a distinct pleasure to appear before you this morning to talk about our efforts in implementing the SAFE Port Act of 2006.

We have worked very closely with our partners in implementing this Act and many of our partners are represented here this morning. I would tell you from the Coast Guard's perspective, just in the year that this Act has been in place, we have already raised the level of port security in our Nation and I feel that increase in port security will continue over the next many years as we bring other elements of the Act into force.

Safety and security are two sides of the same coin and I'd just like to emphasize the point from a Coast Guard perspective that whatever investment we make in security has——

Senator LAUTENBERG. Can you bring the mike a little closer, Admiral, please?

Admiral PEKOSKE.—has a corollary benefit to safety in this Nation. So as we raise our security profile, we've also improved our safety elements and our ability to respond to environmental issues. So safety, security and stewardship are key elements of our efforts in the Coast Guard.

With regard to partnership, I would just like to highlight a couple things and basically reinforce some of the comments that you have already made this morning. My previous assignment was Commander of the First Coast Guard District based in Boston, which had oversight from a flag level of the Port of New York and New Jersey and the partnerships that we have in the Port of New York and New Jersey, like the partnerships we have across the Nation are not only very strong but are absolutely fundamental to our success. We work very closely with Tony Coscia and The Port Authority of New York and New Jersey, the New York City Police Department and the States of New York and New Jersey, plus our industry partners, to improve safety and security in that port.

Assistant Commissioner Winkowski and I have the privilege of jointly chairing inside the Department of Homeland Security, a senior guidance team and the purpose of this team is to bring together Coast Guard operations and Customs and Border Protection operations so that we truly present one face of DHS as we interact with the maritime industry. We have worked very closely on small vessel security. We just had a National Small Vessel Security Summit in June, where we brought together our Federal partners, our State and Local partners and our industry partners to talk about how it is we would raise security with respect to small vessels and where they fit within the entire security profile of our country.

We've also worked very closely on a National Recovery Symposium, which is very critical for us in terms of security and being able to resume commerce in our ports. When you think of the 95

percent of our trade that travels by sea, when there is a transportation security incident, we collectively, between the Federal Government, the State and Local governments and the industry, need to be able to recover those ports as quickly as possible.

We have, from our perspective, have had a very good relationship with the Transportation Security Administration in implementing TWIC. We appreciate Ms. Fanguy's work in that and we just jointly released a press announcement yesterday that announced that beginning on the 16th of October, we will begin enrollment for TWIC in the Port of Wilmington and then 11 more ports over the course of the next month. So that process is now ongoing. And we do appreciate the work of the Government Accountability Office in looking at our efforts to implement this important Act.

A couple of things I'd like to highlight for you is, we've improved already our maritime domain awareness but we have a very significant improvement to that coming up on the first of January 2008, where we will implement long range tracking, which will give the United States visibility of any ships that have declared they're entering the United States or they are within a 1,000 miles of our coastline. So this will be a significant improvement in maritime domain awareness.

We have also worked very hard at the Interagency Command Center issue. We have some very successful Interagency Command Centers. But Senator Cantwell, as you mentioned, this is a very significant resource challenge for us. We sent a report up to the Congress, consistent with the SAFE Port Act requirements that detailed a cost of about $260 million to stand up integrated command centers in the most important ports in our country. That resource challenge is significant for us. We've had some very good successes in the Integrated or Joint Command Centers that we have throughout the country. We've learned a lot about that and once we get the funding for these command centers, I'll look forward to being able to provide that all-hazard, all threat response capability in our ports in this country.

Mr. Chairman, that concludes my opening statement and I would be most pleased to answer any questions the Committee has. Thank you, sir.

[The prepared statement of Rear Admiral Pekoske follows:]

PREPARED STATEMENT OF REAR ADMIRAL DAVID P. PEKOSKE, ASSISTANT COMMANDANT FOR OPERATIONS, U.S. COAST GUARD, DEPARTMENT OF HOMELAND SECURITY

Good morning, Mr. Chairman and distinguished Members of the Committee. I am Rear Admiral David Pekoske, Assistant Commandant for Operations, U.S. Coast Guard. It is a pleasure to appear before you today to discuss the Coast Guard's efforts in implementing the Safety and Accountability for Every Port (SAFE Port) Act requirements 1 year after its implementation.

The objective of the SAFE Port Act is "to improve maritime and cargo security through enhanced layered defenses." The Coast Guard is cited as one of the primary organizations identified with specific responsibilities for implementing this overall objective. Several components within our organization have been involved in achieving the requirements since October 13, 2006 and I will address the SAFE Port Act requirements section-by-section.

We have had many successes to date in meeting the requirements of the SAFE Port Act, including requirements involving the inclusion of Salvage Response Plans in Area Maritime Transportation Security Plans (Section 101); Unannounced Inspections of Maritime Facilities (Section 103); the Port Security Training Program (Sec-

tion 113); the Port Security Exercise Program (Section 114); and Foreign Port Assessments (Section 234).

We recognize, however, that there is still work to be done. There are some timeline requirements in the SAFE Port Act that we have not met, including those related to Notice of Arrival for Foreign Vessels on the Outer Continental Shelf (Section 109) and Enhanced Crewmember Identification (Section 110). We are committed to working closely and diligently with our DHS partners to meet these and other requirements of the SAFE Port Act.

Section 101 Area Maritime Transportation Security Plan to Include Salvage Response Plan

Development of Salvage Response Plans within each Area Maritime Security Plan (AMSP) has been integrated into the five-year plan update cycle established by the Maritime Transportation Security Act (MTSA) of 2002. The AMSP update will be performed by Federal Maritime Security Coordinators in consultation with their respective Area Maritime Security Committees and is planned for completion during early summer 2009.

A Salvage Response Plan will be a major element of the U.S. Marine Transportation System (MTS) recovery section of each AMSP and will provide the coordination and procedural foundation to support development of unified command incident action plans under the Incident Command System (ICS) construct when salvage response becomes necessary to facilitate resumption of trade. Authorities, capabilities, and other salvage issues are currently being coordinated with government and other partners. Consultation with national-level salvage industry representatives is continuing with the development of a Memorandum of Understanding (MOU) between the Coast Guard and the American Salvage Association. The MOU will establish a partnership with the goal of strengthening the communication and working relationship between the Coast Guard and the marine salvage and fire fighting industries to improve vessel and personnel safety; enhance national security preparedness and response; promote timely and professional salvage response to marine casualties; and enhance the protection of the environment along our Nation's waterways.

Resumption of commerce and recovery of the marine transportation system (MTS) following a significant disruption is a significant national issue of concern. The Maritime Transportation Security Act (MTSA) 2002 required that the National Maritime Transportation Security Plan include a plan to restore cargo flow following a National Transportation Security Incident (NTSI). The Coast Guard held a National Recovery Symposium at the National Maritime Institute of Technology and Graduate Studies on August 1 and 2, 2006. The symposium was attended by over 150 executive level participants from numerous branches of state and Federal Government, as well as the private sector.

The Coast Guard is currently developing a concept of operations and specific planning requirements and organizational structures to ensure a focus on MTS recovery following a significant disruptive incident. MTS recovery guidance will be harmonized with, and support implementation of, the Strategy to Enhance International Supply Chain Security recently completed by the Department of Homeland Security with Coast Guard and interagency input. Implementation guidance will also harmonize with MTS recovery principles gleaned from Hurricane Katrina lessons-learned that have already been published in the U.S. Coast Guard Incident Management Handbook.

Review of maritime security developments since the implementation of MTSA, MTS recovery lessons from Hurricane Katrina, best Area Maritime Security practices from the field, and an update of MTSA implementation guidance are in progress. Review results to date have formed the basis for revising Navigation Vessel Inspection Circular 09–02 which is used to guide the five-year AMSP update.

Consistent with the overriding requirement to deter, and when necessary, mitigate the effects of Transportation Security Incidents (TSIs), the Coast Guard is working to make AMSP coordination and procedures "all-hazard and transportation disruption" compatible as much as practicable. This, in conjunction with oil and hazardous materials response coverage provided through Area Contingency Plans (ACP), application of Incident Command System (ICS) principles and structures per the National Incident Management System (NIMS), is intended to support an integrated and coherent preparedness approach across all transportation disruptions without requiring additional port-level plans.

Section 102 Requirements Relating to Maritime Facility Security Plans

The Coast Guard recognizes that information on ownership of maritime facilities and the companies that operate them is vitally important to the management of the security posture and the clear delineation of security responsibilities within the

port. Currently, in 33 CFR 104.415(b)(2), 105.415(b)(2), and 106.415(b)(2), the Coast Guard requires a security plan audit whenever the owner or operator of a vessel, facility or Outer Continental Shelf (OCS) facility changes. Should the audit reveal that an amendment to the security plan is necessary, the security officer of the vessel, facility or OCS facility will submit the amendment to the cognizant Captain of the Port or District Commander for approval. Consistent with the requirement in Section 102 of the SAFE Port Act, the DHS Appropriations Act of 2007 requires the Coast Guard to gather ownership information on vessel and facility security plans.

In order to meet the requirements in these statutes, the Coast Guard has initiated a regulatory project to update 33 CFR Subchapter H regulations and will incorporate these new ownership reporting requirements.

Implementation of the Transportation Worker Identification Credential (TWIC) regulations published in January 2007 will meet the requirement in Section 102 for a qualified individual having full authority to implement security actions for a facility to be a citizen of the United States, unless the Secretary waives the requirement after a determination based on a complete background check of the individual. These regulations, found in 33 CFR 105.205(a)(4), require facility security officers (the qualified individuals in the statute) to possess and maintain a TWIC. The security threat assessment conducted as part of the TWIC program involves a complete background check, including a criminal history records check, a legal status check, and an intelligence and terrorist watch list check, to satisfy the relevant mandate within this section. In addition, the Coast Guard is addressing the requirement for Facility Security Officers to be U.S. citizens in the regulatory project to update Subchapter H. A final fee was published on September 28, along with some modifications to the earlier rule.

Section 103 Unannounced Inspections of Maritime Facilities

Currently, Coast Guard policy calls for an annual inspection of each facility, supplemented by periodic spot checks. The FY07 Homeland Security Appropriations Act provided $15M to, among other efforts, fund additional port security inspections. With this funding, the Coast Guard has created 39 new field billets to add to the current 350 facility inspectors. Thirty-seven of these new billets were filled during the 2007 transfer season, and the remaining two are in the process of being filled. The Coast Guard conducted more than 7,500 annual inspections and spot checks of 3,200 facilities in calendar year 2006. We have also applied additional reserve billets this year to increase facility visits and ensure each facility is inspected not less than two times this year. At least one of those inspections will be unannounced.

Section 104 Transportation Security Card

Section 104 of the SAFE Port Act includes a number of statutory requirements relating to the implementation of the TWIC program. The effort to promulgate TWIC requirements through the rulemaking process met its SAFE Port Act deadline of January 1, 2007, with the posting of the TWIC Final Rule. This rule, together with the *Merchant Mariner Credential Supplemental Notice of Proposed Rulemaking* published on January 25, 2007, will allow mariners to apply for or renew merchant mariner credentials through the mail concurrently with the TWIC enrollment process, eliminating travel to Coast Guard Regional Exam Centers and removing duplicative background checks and other application redundancies which exist under each program. Also, the TWIC final rule incorporates a background check process to enable newly hired workers to begin working while awaiting issuance of their TWIC, in accordance with the Act.

The Coast Guard continues to support the Transportation Security Administration's (TSA's) efforts to implement the TWIC program by providing field and industry guidance to assist with compliance and enforcement activities. In addition, the Coast Guard is working closely with DHS and TSA on the pilot program to test the implementation of card readers to provide critical information and lessons to inform a second rulemaking to address TWIC readers. As part of our support for this effort, the Coast Guard, jointly with TSA, charged the National Maritime Security Advisory Committee (NMSAC) to form a working group of maritime industry and biometric technology representatives to propose specifications for TWIC cards and card readers using a contactless (or proximity) interface. The NMSAC presented recommended specifications on February 28, 2007. A notice of availability of the specifications was published in the *Federal Register* for public comment on March 16, 2007 and the notice of availability of the final contactless specification was published in the *Federal Register* on September 20, 2007.

Work continues on several aspects of the TWIC program. The Coast Guard intends to purchase handheld card readers in FY 2008 for use during vessel and facility inspections and spot checks. After the compliance date passes in a given port,

the Coast Guard will use the card readers to randomly check the validity of an individual's TWIC. Also, the provision for newly hired employees to work while they await issuance of a TWIC is in development and on track. The Coast Guard has received stakeholder comments on policy and included them in the form of a Navigation and Vessel Inspection Circular (NVIC) which provides guidance and instruction on how to implement TWIC regulatory requirements for access control on facilities and vessels. This NVIC was published in July 2007.

Section 107 Long-Range Vessel Tracking

The Coast Guard currently meets the intent and requirements of the Act, using the full range of classified and unclassified vessel tracking information available. While the Long Range Identification and Tracking (LRIT) NPRM did not meet the April 1, 2007 deadline, it was published in the *Federal Register* on October 3, 2007. The Act requires the DHS Secretary to establish a long range automated vessel tracking system that meets the following:

- Tracking: Provided for all vessels in U.S. waters equipped with Global Maritime Distress and Safety System (GMDSS) or equivalent satellite technology; and
- International: Consistent with international treaties, conventions and agreements.

Tracking

The SAFE Port Act requirement demands a multi-faceted approach. Using the full range of classified and unclassified vessel tracking info available, including some information purchased from vendors where appropriate, the Coast Guard currently meets and exceeds the tracking requirement of the Act. Currently, sufficient tracking information exists; however more work is needed in processing, display, and training in the use of this information.

International

Our work to establish a system through the International Maritime Organization (IMO) will provide an unclassified global tracking capability in 2008 as a part of an existing IMO convention and give the United States a system that is compatible and interoperable with the global maritime community. The Coast Guard has been working with the IMO since shortly after 9/11 to implement a global tracking system for the types of vessels described in the Act. Following considerable diplomatic efforts, the international agreement to implement such a system was reached last year, and the global tracking system will be in effect at the end of 2008. In the long run, this approach has more advantages to the United States because it applies globally to all the world's ships of the kind described by the Act instead of just those in U.S. waters or vessels intending to make ports call in the United States. Under this system, the U.S. will have access to information for U.S. Flag vessels regardless of their current location, and vessels bound for U.S. ports when they declare intent to arrive. Information on all other vessels will be available whenever a ship is within 1,000 nautical miles of the U.S. coast. The Coast Guard is examining funding strategies for this important international system.

To complement the above activities, the Coast Guard also initiated a rulemaking to implement in Title 33 of the *Code of Federal Regulations* rules that require ships to report identifying and position data electronically. These rules provide guidance to U.S. and foreign ships on how to comply with this new reporting requirement, as well as an additional enforcement mechanism for ships that fail to comply.

Section 108 Establishment of Interagency Operational Centers for Port Security

Section 108 requires a budget and cost-sharing analysis for implementing interagency operations centers. The report required by this Section was submitted in July. It identified the estimated total acquisition cost of upgrading the 24 Coast Guard Sector Command Centers (SCCs), which encompass the Nation's high priority ports, as approximately $260 million. The major cost elements of this five-year project plan include an information management software suite, a sensor package and facility recapitalization.

The establishment of interagency operations centers is currently not funded. In cooperation with the Department of Justice (DOJ), the U.S. Navy, and the DHS Office of Science and Technology, five prototype centers have been established to date. These centers are each configured differently as test beds for concepts, tactics, procedures and equipment. Cost sharing arrangements exist among the various participants.

Designator	Location	Cost-Sharing Agencies
Seahawk Joint Task Force	Charleston, SC	Dept. of Justice/U.S. Coast Guard
SCC*—Joint	Hampton Roads, VA	U.S. Coast Guard/U.S. Navy
SCC—Joint	San Diego, CA	U.S. Coast Guard/U.S. Navy
SCC—Joint	Jacksonville, FL	U.S. Coast Guard/U.S. Navy
SCC—Joint	Seattle, WA	U.S. Coast Guard/U.S. Navy

*Sector Command Center.

Additionally, seven ports have been identified for short and medium term pilot projects to evaluate joint operations design models between the Coast Guard and Customs and Border Protection (CBP). These pilots will include examination of methods for implementation of a virtual command center construct using various collaboration tools for daily coordination and vessel inspection planning.

USCG is developing Command 21 to field the capabilities necessary to create interagency operations centers as required by Section 108. This initiative would establish interagency operational centers for port security tailored to each port and designed to close gaps in port and coastal maritime security. Command 21 would accomplish this by fielding a sensor network and an information system that allows the centers to monitor maritime activities in critical areas. The system would link vital data on vessel history, crew, and cargo to the activities observed.

Command 21 will be designed to:

- Enhance the effectiveness of maritime security and response operations in mitigating risk, including risks associated with small vessels operating in close proximity to critical infrastructure and key resources in port and coastal areas. This enhanced effectiveness will be accomplished through pro-active tactical surveillance and data fusion;
- Improve maritime port and coastal security systems to complement Secure Border Initiative (SBI) Net;
- Improve unity of effort in a multi-agency operations center environment; and
- Accelerate deployment of a net-centric tactical system that implements government-wide enterprise standards for the sharing of situation data and services across multiple interagency domains and Coast Guard systems.

The Coast Guard's experience with interagency operations centers demonstrates that many tangible benefits to improve maritime safety, security, and stewardship can be achieved. Some of these include:

- Cooperative targeting and coordination of intelligence facilitates information sharing;
- Daily field-level coordination breaks down barriers between agencies;
- Collective use of tactical sensors (radars/cameras) saves time, money and effort;
- Cooperative planning improves readiness and efficiency; and
- Sharing of law enforcement information helps reduce criminal activity in the port and cuts off potential funding to terrorist groups.

Future interagency operations could be greatly improved as all partners will be able to:

- *See* maritime activities using port surveillance sensors;
- *Understand* the scene by automatically bringing tactical and intelligence information together; and
- *Share* this tactical data with each other as they work side by side in improved facilities.

Command 21 is designed to publish tactical data in an open standard that allows other systems across multiple DHS and applicable Federal Government domains to subscribe to the information and use according to the individual needs of each agency. It provides the maritime component of the Department of Homeland Security's Secure Border Initiative (SBI). Moving ahead on both fronts will provide collaborative opportunities to leverage critical resources to broaden the impact of both programs toward securing our borders.

Section 109 Notice of Arrival for Foreign Vessels on the Outer Continental Shelf

The regulations for Notice of Arrival for foreign vessels on the Outer Continental Shelf (OCS) have been developed and incorporated into an existing Coast Guard rulemaking project related to OCS activities. This rulemaking, the updating of 33

CFR Subchapter N, "Outer Continental Shelf Activities," already includes Notice of Arrival requirements for foreign vessels operating on the OCS. The Coast Guard has completed evaluation of the proposed regulations and public comments, and is working to expeditiously publish this rule.

Section 110 Enhanced Crewmember Identification

Historically, the Coast Guard advanced the effort to negotiate the international seafarer's identification initiative at the International Labor Organization (ILO), resulting in the ILO–185 Seafarer's Identification Document (SID). However, a requirement within ILO–185 prohibiting implementing nations from requiring a visa for seafarers holding a SID to be eligible for shore leave has prevented the U.S. from ratifying ILO–185.

In accordance with the Act, the Coast Guard has prepared a draft NPRM defining the identification documents necessary for all foreign mariners calling on U.S. ports. The proposed identification requirements would also apply to U.S. mariners arriving at U.S. ports from a foreign port of place of departure.

Section 111 Risk Assessment Tool

The Maritime Security Risk Analysis Model (MSRAM) is being used by Captains of the Ports/Federal Maritime Security Coordinators (FMSCs) and Area Maritime Security Committees (AMSC) to analyze and prioritize scenario-based risks within their areas of responsibility, and to measure risk reduction potential in the evaluation of port security grant program proposals. FMSC and AMSCs are required to validate the MSRAM data on an annual basis. This was last completed in the summer of 2007 using MSRAM version 2.

Section 112 Port Security Grants

The Coast Guard worked with the DHS Office of Grants and Training, who has fiduciary responsibility for the Port Security Grant Program, to complete the report to Congress required by this Section. The report was submitted to Congress on April 27, 2007.

The Port Security Grant Program (PSGP) provides grant funding to port areas for the protection of critical port infrastructure from terrorism. FY07 PSGP funds are primarily intended to assist ports in enhancing risk management capabilities; domain awareness; capabilities to prevent, detect, respond to and recover from attacks involving improvised explosive devices (IEDs) and other non-conventional weapons; as well as training and exercises.

$201,670,000 was available for Port Security Grants in FY07. These funds were divided amongst four tiers of ports. Within Tier I, eight of the highest risk port regions were allocated a fixed amount of funding based on risk. In many cases, multiple port areas were grouped together to reflect geographic proximity, shared risk, and a common waterway. Port areas submitting applications within Tier II and III were eligible to compete for the FY07 PSGP but were not guaranteed funding. Section 112 of the SAFE Port Act also required that any entity addressed in an Area Maritime Security Plan also be eligible to apply. Tier IV was established for those new entities not within the port areas in Tiers I–III. This added approximately 259 ports to the 102 highest risk ports for a total of 361 that were eligible to compete, but were not guaranteed funding.

Funds were awarded based on analysis of risk and effectiveness of proposed investments by the applicants. Risk to port Infrastructure Protection Program Detail areas was assessed using a methodology consisting of threat, vulnerability, and consequence factors. The majority of port security grant funds—$120.6 million—was allocated to eight Tier I ports or port areas that we consider to be the highest risk.

Grant applicants had 60 days from January 6, 2007 to complete this process for the remaining $81M. Applications were required to be submitted electronically via the *grants.gov* website no later than March 6, 2007. The initial reviews were completed by the local Captain of the Port in conjunction with the Maritime Administration's (MARAD's) regions. These results were forwarded to a national review panel comprised of representatives from the Coast Guard, the Transportation Security Administration (TSA), DHS Infrastructure Protection (IP), Grants and Training (G&T), the Domestic Nuclear Detection Office (DNDO), and MARAD that convened on April 9, 2007. The results were announced on May 30, 2007.

The $110 million was provided by Congress in supplemental Port Security Grant Funding (P.L. 110–28, the U.S. Troop Readiness, Veterans' Care, Katrina Recovery, and Iraq Accountability Appropriations Act, 2007). Using the same risk-based analysis utilized during the initial FY07 Port Security Grants, funds were allocated to Tier I and II ports to develop a Port-Wide Risk Management/Mitigation and Business Continuity/Resumption of Trade Plan which will identify a prioritized listing of items to be addressed within future grant applications. Tier III ports that pre-

viously submitted projects under the initial FY07 PSG Program which were validated but unfunded, are to be funded with the Supplemental Grant. Tier IV ports also applied for TWIC and Training under the Supplemental Grant funding. The application period has closed. Both field and national review of the Supplemental applications have been completed, and announcement of awards were made by September 30, 2007.

Section 113 Port Security Training Program

The Coast Guard is supporting the FEMA National Preparedness Directorate's National Integration Center through Training and Exercises Integration (formerly known as the DHS Preparedness Directorate, Office of Grants and Training Division). Collectively, we are making progress in establishing the program delineated in the Act. There are a number of existing initiatives and new initiatives that will address the requirements in this section.

In response to Congressional mandate, the Coast Guard and MARAD developed model courses for the training of facility and other personnel to meet the requirements of the Maritime Transportation Security Act of 2002. These model courses establish a competence based standard and contain most of the requirements under this Section of the Act. The model courses were developed in support of the facility security plan requirements, and apply to all personnel working in a port facility or required to enter a port facility in response to an emergency. These model courses are available via website to Federal, state and local personnel from the public and private sector and they are undergoing a review to include lessons learned and the additional topics required under the Act. To ensure quality training, Coast Guard and MARAD developed and implemented a voluntary course acceptance and certification process using the model courses as the guidelines for acceptance. The Coast Guard is currently revising the regulations for security training for facility personnel to ensure all training is measured against a standard of competence, including the topics required under the SAFE Port Act.

The FEMA National Preparedness Directorate's National Integration Center, through Training and Exercises Integration, has awarded a $6.18 million Cooperative Grant to the Florida State University to develop courses meeting the Maritime Transportation Security Act of 2002 requirements (model courses), and covering the eight port security-related topics required under the Act. MARAD and the Coast Guard are actively assisting DHS to ensure this training will be consistent with existing standards and will provide the maximum possible return on investment. It is envisioned that these courses will be available for in-classroom and on-line training; and will be available both to Federal, state and local personnel as well as members of the private sector who work in the port security realm.

In addition, the FEMA National Preparedness Directorate's National Integration Center, through Training and Exercises Integration, has made available other training courses that address individual port security topics required under the Act. These courses are provided to State and local emergency responders and other identified audiences by Training and Exercises Integration, and are coordinated by each State's Governor-designated Training Point of Contact.

Section 114 Port Security Exercise Program

Current port security exercise programs conduct live, risk-based exercises that are realistic and evaluate total capability by focusing on the port community, in order to evaluate the entire capability. These exercises involve State and local governments, as well as facilities and vessels, to ensure that consistent methodology is applied and that all requirements are met as a result. Although current programs do not mandate facility participation in these annual exercises, participation has been strong and continues to increase. Facilities, as well as vessels, are encouraged to observe and/or participate in these port security exercises. When they choose to participate, they are offered the opportunity to put forth exercise objectives tailored to meet their specific needs.

Since January 2005, the Coast Guard has assisted TSA in implementing their Port Security Training and Exercise Program (PortSTEP). Similarly, since October 2005, the Coast Guard has sponsored its own Area Maritime Security Training and Exercise Program (AMStep) that exercises the port stakeholder's ability to implement the provisions of the Area Maritime Security Plan. The Coast Guard and TSA have synchronized AMStep and PortSTEP to maximize coverage across the U.S. and minimize duplication of effort. In FY07, these two programs collectively sponsored 41 port security exercises. Exercise types have included basic and advanced tabletop, discussion-based exercises to full-scale, operations-based exercises. The type of exercise and scenario selected are collectively decided upon by Area Maritime Security Committee (AMSC) members, through application of their most current risk-

based port assessment and assessment of preparedness needs. The results of both these exercise programs and all lessons learned, best practices, and corrective actions are documented in a semi-annual report to Congress.

The "Training" aspect of current port security exercise programs focuses on the National Incident Management System (NIMS) Incident Command System (ICS). Training, such as I–200 (Basic), I–300 (Intermediate) and I–320 (Team training), is offered to the entire port community prior to each annual exercise. Security-specific training is provided from within the port community.

Initial performance measures for port security exercises were established under Coast Guard NVIC 09–02, Change 2. These measures, outlined as objectives, are currently being revised by the Coast Guard to align with MTSA requirements to test the AMSPs and with the Homeland Security Exercise and Evaluation Program. All Lessons Learned, Best Practices, and Remedial Action Items are captured in the Coast Guard's Contingency Preparedness System (CPS), which can be accessed by the entire Coast Guard. Additionally, through the use of Homeport, the Coast Guard's communications and collaborations Information Technology application, Lessons Learned and Best Practices, can be made available to the entire port community (Federal, state, local, tribal and industry).

Although AMStep is currently being carried out under contract support, the Coast Guard has begun the hiring of personnel to staff National-level and Regional-level exercise support teams. These teams will assist Coast Guard Sector Commands (port-level) and Districts with the following contingency exercise programs: port security, oil/hazardous substance response, natural disaster, mass rescue, alien migration interdiction, civil disturbance, counterterrorism, military outload, combatant commander support, and physical security/force protection. This is an "All Threats/All Hazards" approach.

Section 115 Facility Exercise Requirements

Current regulations in 33 CFR 105.220(c) require facilities to conduct an annual exercise. These exercises may include either live, tabletop, or participation in a non-site-specific exercise. In order to meet the requirement in Section 115, the Coast Guard has initiated a regulatory project to update 33 CFR Subchapter H regulations and will incorporate definition of "high risk facility" and the requirement for high risk facilities to conduct bi-annual full-scale exercises.

Section 128 Center of Excellence for Maritime, Island and Extreme/Remote Environment Security

The Coast Guard is assisting the DHS Science and Technology (S&T) Directorate to meet the requirements of Section 108. The Broad Area Announcement (BAA) for a Center of Excellence (COE) for Maritime, Island and Extreme/Remote Environment Security was announced at the beginning of February 2007. This BAA incorporated Maritime Domain Awareness (MDA) study as a central component of a broader system of research into maritime security. This solicitation is still open, and there has been good response from the academic community. DHS S&T expects to award the COE by the end of 2007. The Coast Guard looks forward to this important new research component that will support DHS.

Section 201 Strategic Plan to Enhance the Security of the International Supply Chain

The Coast Guard assisted the Department of Homeland Security's authoring team in drafting the required Strategy to Enhance International Supply Chain Security, providing lead authors for sections on response and recovery. Looking forward, the Coast Guard is working to structure the first required five-year update to Area Maritime Security Plans (AMSPs) to position them to support field-level implementation of the strategy as it pertains to Transportation Security Incidents (TSIs). A planning objective is to make these community-based coordination arrangements and procedures compatible for application during other forms of transportation disruption, insofar as practicable. We assigned the same Coast Guard subject matter experts to support each initiative, thereby facilitating content alignment for this purpose.

Section 233 International Cooperation and Coordination

The Coast Guard has been working with a variety of international organizations including the Asia Pacific Economic Cooperation (APEC) Forum, the Group of Eight (G8), and the Organization of American States (OAS) to conduct capacity building activities to improve the port security regimes of developing countries. Coast Guard representatives serve on maritime security expert groups of these organizations and have been intimately involved in identifying and executing projects. Furthermore, the Coast Guard had been working cooperatively with the Departments of State and Defense in various security assistance activities.

Of particular note is our work with the OAS, an organization that is specifically mentioned in the SAFE Port Act for close coordination. Through the Inter-American Committee on Counter-Terrorism (an OAS body), and in conjunction with Canada, the Coast Guard is developing a series of exercises and best practice conferences. The first port security exercise was completed in Argentina in September 2007.

Modeled after the North Pacific Coast Guard Forum, which has had some notable successes in the area of joint operations recently, the new North Atlantic Coast Guard Forum will leverage bilateral relationships and encourage partner-based activities in the Atlantic theater. Its first meeting is scheduled for 22–25 October in Stockholm, Sweden.

Section 234 Foreign Port Assessments

The Coast Guard has increased the pace of assessments and is on track to complete an initial assessment of all of our trading partners by March 2008. The Coast Guard intends to conduct assessments on a 2-year cycle thereafter.

This 2-year cycle is consistent with the guidance contained in the FY07 DHS Appropriations Act, which called on the Coast Guard to double the rate of assessments (basically from three per month to six per month). This reassessment cycle actually exceeds the requirement of the SAFE Port Act which call for reassessments to be conducted on a 3-year cycle. Additional resources (approx. $6.7M and 32 FTE) provided in the FY07 DHS Appropriations Act support this increase in activity.

Section 303 Research, Development, Test, and Evaluation Efforts in Furtherance of Maritime and Cargo Security

DHS and the Coast Guard have current and planned efforts to support the furtherance of maritime and cargo security. The Coast Guard RDT&E efforts for FY07 include:

Mission Areas	Programs/Projects
Boarding Team Support and Communications	1. Maritime Biometrics, ID at Sea 2. Boarding Team Connectivity 3. Next Generation Underway Connectivity 4. Boarding Officer Tools and Equipment Support
Compel Compliance	1. Anti-Personnel 2. Stopping Mid-Sized Vessels
Platforms and Sensors	1. Acoustic Buoy 2. Multi-Sensor Performance Prediction 3. Global Observer 4. Small UAS Evaluations
Sector and Port Security Operations	1. Maritime Domain Awareness Community of Interest 2. National Automatic Identification System
Miscellaneous	1. Net-Centricity 2. Weapons of Mass Destruction

The Coast Guard projects funded by DHS Office of Science and Technology (S&T) FY07 funds include:

Mission Areas	Programs/Projects
Boarding Team Support and Communications	1. Boarding Team Communications
Sensor, Data Fusion, and Decision Aids (Maritime)	1. Visualization Tools 2. Hawkeye Watch keeper Prototype 3. Offshore Buoys for Vessel Detection 4. Emergence Response Blue Force Tracking 5. Swimmer/Diver Detection 6. Global Observer

DHS S&T FY08 funding has yet to be defined. The Coast Guard is planning a comparable dollar figure to support the furtherance of maritime and cargo security in FY08.

Conclusion

In conclusion, the Coast Guard is committed to implementing the Security and Accountability for Every Port Act. We continue to make headway on all fronts and look forward to future progress and partnerships with international, Federal, state,

and local port organizations. Thank you for the opportunity to testify before you today. I will be happy to answer any questions you may have.

Senator LAUTENBERG. Thank you. Ms. Fanguy?

STATEMENT OF MAURINE SHIELDS FANGUY, PROGRAM DIRECTOR, TRANSPORTATION SECURITY ADMINISTRATION, DEPARTMENT OF HOMELAND SECURITY

Ms. FANGUY. Thank you. Good morning, Mr. Chairman, Vice-Chairman Stevens and distinguished Members of the Committee. My name is Maurine Fanguy and I'm the Program Director for the Transportation Worker Identification Credential Program, also known as TWIC. Today, I'm here to show you the results of our efforts, the TWIC Credential.

In all of our previous meetings, we have talked to you about what we needed to do and what we were going to do. Now I would like to tell you what we have done. This is my TWIC card. Last week, I went to Wilmington and I enrolled. On October 16, less than 2 weeks from today, Wilmington's port workers will begin enrolling for their TWICs. This card represents the completion of TWIC's flight-testing.

Just like I did, Wilmington's port workers will come to our enrollment center and give their personal information and fingerprints to a trusted agent for vetting. Their cards, just like mine, will be printed and sent back to Wilmington for activation.

TWIC is one of the world's most advanced interoperable, biometric credentialing programs, powered by state-of-the-art technologies. Once TWIC is up and running, TSA will vet as many workers in 1 day as we did in 1 year of the prototype. That's over 5,000 workers a day. This program will impact the livelihoods of the hundreds of thousands of American workers who represent the backbone of global commerce.

While the start of enrollment represents a significant milestone in the program, more importantly, it is a critical step in our multi-layered approach to securing our Nation's ports. Since Assistant Secretary Holley testified in April, we have completed testing and have made advances in all aspects of the program. First, we added 17 new TWIC enrollment sites, based on stakeholder input. We understand the importance of making enrollment as convenient and accessible as possible. The additional sites bring the total number of fixed enrollment centers to 147 nationwide. We have also added a mobile enrollment capability to take TWIC to the workers. Second, we reduced the price of a standard TWIC card to $132.50. It's very important to us to limit the cost to workers as much as possible. Third, we published technical specifications for TWIC biometric card readers. This allows industry to enhance access control technologies used at 3,200 facilities and on 10,000 vessels. And fourth, we held kick-off meetings with five card reader pilot participants, the Port Authorities of New York and New Jersey or New Jersey and New York, Mr. Lautenberg, Los Angeles, Long Beach and Brownsville as well as Watermark Cruises in Annapolis, were selected to represent a broad range of operating environments. We are continuing to meet with interested stakeholders to identify additional participants.

After successful startup in Wilmington, we will proceed to Corpus Christi in early November. By mid-November, enrollment will start in Baton Rouge, Beaumont, Honolulu, Oakland and Tacoma. This group will be followed in late November by Chicago Calumet, Houston, Port Arthur, Providence and Savannah. As we begin enrollment at these ports, we will continue to release more information about the rest of the 147 ports where we will begin enrollment.

We look forward to the start of enrollment on October 16. For the first time, thousands of ports and vessels will have one interoperable security network with workers holding a common credential that can be used across that entire network. We will continue to work with our partners, the Coast Guard, maritime stakeholders and this Committee to ensure the ongoing success of the TWIC program.

Thank you for the opportunity to appear today and I would be happy to answer any questions.

[The prepared statement of Ms. Fanguy follows:]

PREPARED STATEMENT OF MAURINE SHIELDS FANGUY, PROGRAM DIRECTOR, TRANSPORTATION SECURITY ADMINISTRATION, DEPARTMENT OF HOMELAND SECURITY

Good morning, Chairman Inouye, Vice Chairman Stevens and distinguished Members of the Committee. Thank you for this opportunity to share with you the significant progress we have made on the Transportation Worker Identification Credential (TWIC) program. I would like to acknowledge the leadership this Committee has provided in defining the vision for TWIC.

The TWIC program is moving aggressively toward its objectives while making sound programmatic decisions focused on enhancing port security. I am happy to inform the Committee that enrollment will begin in Wilmington, Delaware later this month.

There have been a number of critical advances in the program since last spring:

- Completing test milestones on the enrollment system
- Adding TWIC enrollment sites based on stakeholder input
- Reducing the price of a TWIC card
- Establishing reader technical specifications
- Identifying card reader pilot participants and holding kick-off meetings

Completing Test Milestones on the Enrollment System

TWIC will impact the livelihoods of hundreds of thousands of American workers essential to the smooth flow of global commerce. Once TWIC is up and running, TSA will vet as many workers in one day as we did during the entire year-long prototype. The importance and enormity of this task within the maritime environment, with a dynamic and mobile workforce, has demanded a methodical approach with rigorous testing.

TWIC will be one of the world's most advanced, interoperable biometric credentialing programs and is powered by state-of-the-art technologies. We are nearly complete on our "flight test" of the full TWIC system, which has five main components:

- *Pre-Enrollment Web Site:* allows workers to schedule appointments and provide information ahead of time to make enrollment easier.
- *Enrollment Center:* captures a worker's biometric and biographic information and submits the information for security processing.
- *TWIC Core System:* routes applicant information for processing, conducts data integrity checks, and manages the status of TWIC cards.
- *Screening Gateway:* aggregates security threat assessment data from the FBI, Citizenship and Immigration Services, and watchlists. It is important to note that the Screening Gateway is used across all of TSA's vetting programs.
- *Card Production:* electronically loads an applicant's information onto a TWIC smart card and then physically produces the card.

All five of these parts were first tested individually. Next, these pieces were integrated to ensure the functionality of the end-to-end process of conducting accurate and timely security threat assessments and producing high quality credentials. In addition, security and privacy requirements were validated throughout the process. After our contractor verified system readiness, TSA completed independent verification before beginning final test enrollments in the field using live vetting on government and trusted contractor personnel.

Today we are in the final stages of field testing. The switch has been turned on and once field testing is completed, we will open the doors and begin enrollment in Wilmington, Delaware. After we verify successful enrollment operations in Wilmington, we will move forward aggressively to expand TWIC across the Nation.

Adding TWIC Enrollment Sites

The TWIC final rule established a network of 130 enrollment sites located across the Nation. Through collaboration with maritime stakeholders, we understand the importance of making enrollment as convenient and accessible as possible. We also have worked with the Department and our partners in the United States Coast Guard to reach out to stakeholders in the field and have identified additional locations for TWIC enrollment centers. At this time, we will field 146 fixed enrollment centers. In addition, we have worked with our contractor to add a mobile enrollment capability to take TWIC to the workers.

Reducing the Price of a TWIC Card

TWIC is a fee-based program paid for by applicants. We fully realize that these costs are significant and we are mindful of the need to identify areas for cost reduction. Recently, we announced that the fee for a standard TWIC will now be $132.50, a decrease from the price anticipated in the Final Rule. Workers with current, comparable threat assessments including HAZMAT, Merchant Mariner Document (MMD) or Free and Secure Trade (FAST)) will receive a discounted fee of $105.25. The cost of a lost, damaged or stolen credential is $60.

Establishing Reader Technical Specifications

The TWIC technical architecture is compatible with the credentialing standards established in Federal Information Processing Standard (FIPS) 201–1. This alignment is critical to support card and reader interoperability within the maritime mode. In response to comments received on the initial TWIC Notice of Proposed Rulemaking, TSA and the Coast Guard decided to remove the requirement for biometric readers from the TWIC final rule to allow time to establish technology specifications to support maritime operations.

TSA and the Coast Guard sought the advice of the National Maritime Security Advisory Committee (NMSAC) which established a working group to collaboratively develop new technical specifications that complement FIPS 201–1 and add features that will support high-volume physical access in the harsh maritime environment. The working group included representatives from both the maritime and technology industries.

TSA recently published the TWIC reader hardware and card application working technical specification. The working specification establishes the requirements for biometric card readers for the pilot projects required by the SAFE Port Act. These readers will be tested during the pilot program. As the card and readers are envisioned to operate when TWIC is fully implemented, use of a PIN will not be necessary to release the biometric, unless the owner/operator chooses to use contact readers and the contact side of the credential.

Identifying Card Reader Pilot Participants and Holding Kick-Off Meetings

As required by the SAFE Port Act, we have initiated pilot programs with five partners across the country to test card readers. The pilots will test access control technologies in real world marine environments. Our current list of participants includes the Port Authorities of Los Angeles, Long Beach, Brownsville, and New York/New Jersey, in addition to Watermark Cruises in Annapolis, Maryland. As part of the outreach efforts for the TWIC program and the Department's Port Security Grant Program, we continue to seek additional participants. Our objective is to include pilot test participants that are representative of a variety of facility vessels which operate in a variety of geographic locations and environmental conditions. There appears to be sufficient interest from the maritime community to achieve this objective.

We are in the process of finalizing the test approach for the pilots. We are working with DHS Science and Technology and the National Institute of Standards and Technology (NIST) to establish a test plan that will evaluate the card-reader interface under a variety of conditions and assess its impact on operations. Through the

pilot tests, we will investigate the impacts of requiring biometric identity verification on business processes, technology, and operational impacts on facilities and vessels of various size, type, and location. As the program proceeds, the pilots will inform the TWIC reader rulemaking process and ultimately result in final regulations that require the deployment of transportation security card readers consistent with the findings of the pilot program.

Lessons Learned and Future Efforts

We are proud of the significant progress we have made in the past 6 months and are mindful of the challenges ahead. As we move forward in the TWIC program, we are committed to incorporating our lessons learned to drive sound management decisions geared at improving all aspects of the program, including:

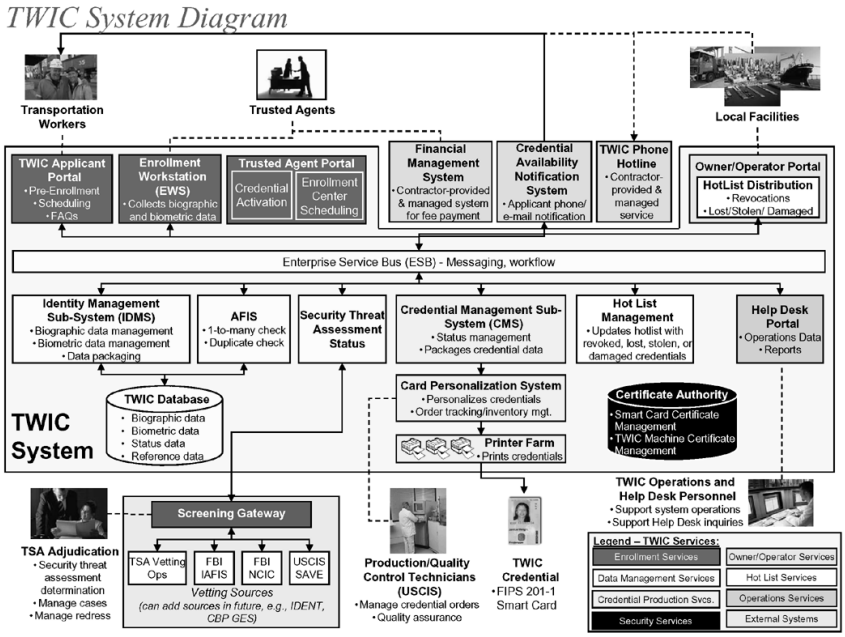
- *Look for efficiencies by eliminating duplicative regulatory processes.* TSA and Coast Guard are developing procedures for the sharing of fingerprints, identity verification, criminal history, and photographs for TWIC which is expected to save not only money but time. In addition, merchant mariners will no longer be required to visit a Regional Exam Center to obtain and renew their credentials, resulting in substantial time and travel savings.
- *Place the highest value in stakeholder input; it is time well spent.* The public hearings, comments to the NPRM, meeting with operators and associations, and contributions of advisory councils all added great value. We came away from each and every one of these efforts better informed about the challenges, the unacceptable impacts, and the practicable options for protecting our ports.
- *Address the impact on small businesses.* TSA and the Coast Guard worked closely with the Small Business Administration to minimize the financial and operational impact on small businesses wherever possible. The rule includes provisions that allow MTSA-regulated passenger vessels (excluding cruise ships) to establish employee access areas for crewmembers that do not require unescorted access to secure areas such as the pilot house and engine room. This provision reduces the impact on those employees who rarely need to use spaces beyond those designated for support of passengers while maintaining the integrity of vessels' secure areas. We are also producing and distributing a Small Business Compliance Guide to assist small businesses in their implementation of the program.
- *When practical, preserve state regulatory flexibility.* Mariner regulations and port security plans preempt state regulations. However, the TWIC regulations do not preempt states from requiring background checks and badging systems for non-security purposes in addition to TWIC. States may need to set standards for important purposes other than terrorism threats, such as theft or organized crime.
- *Plan for privacy.* All data collected at an enrollment center will be completely deleted from the enrollment center work stations after transmission to TSA. The entire enrollment record (including all fingerprints collected) is stored in the TSA system, which is protected through role-based entry, encryption, and segmentation to prevent unauthorized use. No paper records with personal identification information are created in the enrollment process.
- *Technical innovation requires adaptive contract management.* TWIC is attempting to develop a 21st century technology that accommodates evolving IT standards suited to emerging needs that span local, international, public, and private interests. This requires continual reevaluation of the scope and methods of contracting. The recent Lockheed Martin performance-based contract award is a culmination of our efforts to date. We will continue to look for and implement adaptive program planning, contractor oversight, and metrics to ensure the success of the program.
- *Plan to address what issues may arise during testing.* Evolving technology, such as card readers, create a changing environment and program control constraints. This is especially the case when the technology must be deployed to a vast multitude of entities with remote connectivity challenges (*e.g.,* vessels) and varying degrees of access control system capabilities.

Conclusion

The steps we are taking will be an extremely important aspect to the security of our port facilities and vessels. TSA will continue to work with our partners, the U.S. Coast Guard and maritime stakeholders, to ensure that for the first time in history thousands of independent businesses will have one, interoperable, security network

and workers will hold a common credential that can be used across that entire network.

I appreciate the keen interest that this Committee has in an effective implementation of TWIC, and I thank you for your support. Mr. Chairman, this concludes my testimony and I am pleased to answer any questions that you may have.



Senator LAUTENBERG. Thank you. Mr. Winkowski?

STATEMENT OF HON. THOMAS S. WINKOWSKI, ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, U.S. CUSTOMS AND BORDER PROTECTION

Mr. WINKOWSKI. Thank you, Mr. Chairman and good morning to everybody and the distinguished Members of the Committee and Mr. Vice Chairman. Thank you for this opportunity to discuss with you today the status of U.S. Customs and Border Protection's efforts since the passage of the SAFE Port Act nearly 1 year ago. As the Assistant Commissioner for almost 3 months now, I can report the CBP has taken strong actions in order to be responsive to this piece of significant legislation.

I would first like to thank the Congress for your continued interest in the important subject of maritime and supply chain security. In many ways, I look at Congressional passage of the SAFE Port Act as an endorsement of CBP's approach to cargo security begun after the events of 9/11. As you know, CBP has developed and implemented unprecedented initiatives to achieve our twin goals of strengthening the security of cargo entering our borders and facilitating the flow of legitimate trade and travel.

CBP uses a multi-layered approach to ensure the integrity of the supply chain from the point of container stuffing through vessel arrival at a U.S. port of entry. This multi-level approach includes the use of trained CBP officers, technology, automation, electronic in-

formation and partnerships with the trade agencies in foreign governments.

I'm sure you are already familiar with many of our initiatives and programs as they have been critical components of our strategy for a number of years. However, I wanted to highlight some important accomplishments that demonstrate how far we have come since September 11 and provide insight on some of the efforts the CBP has made over the last 12 months to meet the requirements of the SAFE Port Act. CBP, through the Container Security Initiative and in coordination with the Department of Energy's Mega-Port Program has partnered with other countries to deploy personnel and technology in an effort to prevent terrorists and terrorist weapons from entering the United States.

Today, CSI is operational in 58 ports covering 85 percent of the maritime containers as cargo shipped to the United States. At these 58 locations worldwide, CBP officers and ICE agents, working along side their host government counterparts, identify the highest risk cargo and perform examinations before the cargo is laid onboard a vessel destined to the United States. This is significant progress.

CBP continues to enhance and improve upon this program, as the Secretary of Homeland Security announced, the Secure Freight Initiative on December 7, 2006. This first phase of the Secure Freight Initiative creates an unprecedented partnership with Pakistan, Honduras and the United Kingdom, Oman, Singapore, Korea and Hong Kong and will provide these governments with a greater window into potentially dangerous shipments moving through their seaports. In Port Qasim, Port Cortes and Southhampton, the deployed scanning equipment will capture data on all containers bound to the United States, and filling the pilot requirements set up by Congress in the SAFE Port Act.

Surpassing these Congressional requirements, DHS has also partnering with some of the world's largest container ports. The size and complexity of larger ports, such as Singapore, Hassan and Hong Kong required initial limited deployment. This first phase will provide lessons learned and evidence of how this new integrated technology can meld smoothly into the logistics operations and risk management process while complimenting the flow of commerce at each different port.

DHS will submit reports to Congress in February and April 2008, detailing the progress made under SFI. This report will also outline the successes and challenges associated with implementation of 100 percent scanning in foreign locations, including issues related to the availability, the capabilities and efficiency of technology and equipment, the process of negotiations and discussions with host nation counterparts as well as foreign input and feedback, the impact on the movement of cargo through ports and across the global supply chain, the staffing and human capital requirements that will be necessary, both abroad and domestic and numerous additional considerations. The data, experience and lessons learned from the initial phase of SFI will provide necessary insight into the practicality and benefits of 100 percent scanning and will certainly guide in decisions regarding the possible expansion of SFI.

On one of the key components of CBP's layered defense is the advance electronic cargo information required on all modes of transportation by the Trade Act of 2002, including a 24-hour rule for maritime cargo. The SAFE Port Act mandated a provision of additional data elements for improved high-risk targeting and the overall enhancement of the Automated Targeting System, working actively with the trade through the COAC CBP developed and processed a new secure security filing, better known as "10 plus 2" in an effort to obtain additional advance cargo information and enhance our ability to perform risk-based targeting. Under this initiative, the importer or its designee agent will file 10 new unique data elements, not currently provided to C–TPAT while carriers will provide stow plan data and container status messages. On the C–TPAT, another premiere program that we have, we're on target from the standpoint of the mandates of the SAFE Port Act and our RPM and NII technology, we continue to make tremendous inroads in ensuring that large pieces of—large freight is brought through our RPM. So with that, Mr. Chairman, I conclude and look forward to your questions.

[The prepared statement of Mr. Winkowski follows:]

PREPARED STATEMENT OF HON. THOMAS S. WINKOWSKI, ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, U.S. CUSTOMS AND BORDER PROTECTION

Introduction

U.S. Customs and Border Protection (CBP) appreciates this opportunity to discuss with you today the Security and Accountability For Every Port Act (SAFE Port Act) and the efforts of CBP nearly one year after its passage.

It is noteworthy that CBP worked quite closely with the House and Senate in the development of the SAFE Port Act and applaud the high level of Congressional interest in securing United States ports and the global supply chain. Much of what is in the SAFE Port Act codified initiatives that the U.S. Customs Service, now CBP, undertook immediately after 9/11 and has been implementing successfully ever since.

Below are updates on the primary areas of activity being undertaken by CBP to fully implement the Act.

Container Security Initiative (CSI)

To meet the priority mission of preventing terrorists and terrorist weapons from entering the United States, CBP has partnered with other countries through the Container Security Initiative (CSI) to deploy multi-disciplined teams to selected foreign seaports to identify cargo containers that pose a potential risk for terrorism and inspect those containers at the foreign ports before they are shipped to the United States. CSI is an example where the SAFE Port Act codified existing DHS programs, and CBP is in compliance with the Act's mandates.

Almost 32,000 seagoing containers arrive and are off loaded at United States seaports each day. In Fiscal Year 2006, that equated to 11.6 million cargo containers annually. Because of the sheer volume of sea container traffic and the opportunities it presents for terrorists, containerized shipping is uniquely vulnerable to terrorist exploitation. CSI's effectiveness and successes can be measured by several factors. At its core is the cooperation and information sharing between the CBP officers in the foreign seaports and the host government personnel. Additionally, CSI has been instrumental in enhancing port security. Through CSI, many foreign ports that previously did not utilize or possess non-intrusive inspection (NII) equipment now have either purchased their own or have access to NII equipment. Additionally, CSI has partnered with Department of Energy's Megaports Initiative at several CSI ports to further enhance the host nation's capability to screen cargo for nuclear and other radioactive materials that could be used by terrorists against the United States or a host country. This fiscal year CSI expanded to 8 additional ports, and reached a milestone of 58 ports worldwide covering 85 percent of the container traffic destined to the United States. This is significant progress.

Secure Freight Initiative (SFI) and 100 Percent Scanning

Building upon the success of the Container Security Initiative (CSI), on December 6, 2006, the Secretary of Homeland Security, in cooperation with the Department of Energy (DOE), Department of State (DOS) and with the maritime industry and foreign government partners, announced Phase One of the Secure Freight Initiative (SFI). SFI is an unprecedented effort to build upon existing port security measures by enhancing the United States Government's ability to scan containers for nuclear and radiological materials in seaports worldwide and to better assess the risk of inbound containers.

The initial phase of the SFI involves the deployment of a combination of existing technology and nuclear detection devices to three ports as per the requirements of the SAFE Port Act, but will also extend, in limited operation, to four additional foreign ports. This will provide a more complete analysis for SFI by including different operational and geographic settings at each port and will provide exposure of different models for future 100 percent scanning. SFI Phase I Ports include: Port Qasim, Pakistan; Port Cortes, Honduras; Southampton, United Kingdom; Port Salalah, Oman; Brani Terminal at Port of Singapore; Gamman Terminal at Port Busan, Korea; and the Modern Terminal in Hong Kong. SFI Phase I is currently on schedule to begin operations at the three ports required by the SAFE Port Act.

This first phase will provide lessons learned on how this new, integrated technology can meld smoothly into the logistics, operations, and risk management process while complementing the flow of commerce at each different port. Additionally, this first phase of SFI will provide the partnering governments with a greater window into potentially dangerous shipments moving through their seaports. Secure Freight will provide carriers of maritime containerized cargo with greater confidence in the security of the shipment they are transporting, and it will increase the likelihood for shippers and terminal operators that the flow of commerce will be both uninterrupted and secure. SFI will use the latest scanning technology, however data analysis, using the Automated Targeting System, will continue to be our primary method in screening containers.

The lessons learned and experience gained from Phase One represent critical steps in the process of determining whether the concept of 100 percent overseas scanning is technologically and economically feasible and the degree to which it increases the security of the international supply chain.

DHS will submit reports to Congress in February and April 2008 detailing the progress made under SFI. These reports will also outline the successes and challenges associated with the implementation of 100 percent scanning in foreign locations, including issues related to the availability, capabilities and efficiency of technology and equipment; the process of negotiations/discussions with host nation counterparts as well as foreign input and feedback; the impact on the movement of cargo through ports and across the global supply chain; the staffing and human capital requirements that will be necessary both abroad and domestically and numerous additional considerations.

Domestic Radiation Detection and Imaging

The SAFE Port Act requires that a deployment strategy plan be developed for the placement of radiation portal monitors (RPMs) throughout the Nation's ports of entry. That plan has been submitted to Congress by the Department.

CBP began deploying RPMs in October 2002, with the first deployment at the Ambassador Bridge in Detroit. Since that time, CBP and the Domestic Nuclear Detection Office (DNDO) have deployed over 1,000 RPMs at mail facilities, seaports, and land border crossings and will deploy the first RPM in the air cargo environment by the end of calendar year 2007. Specifically, the SAFE Port Act mandates that all containers entering through the top 22 seaports be scanned for radiation. Currently, the Department has deployed radiation detection equipment to each of these 22 ports. Due to unique operational considerations at some of these ports, not every terminal within a port is currently equipped with such equipment. However, to satisfy the requirements of the SAFE Port Act and to further enhance port security, CBP and DNDO continue to work with these considerations, and by the end of this calendar year will scan approximately 98 percent of all containerized cargo at these 22 seaports.

With the additional deployment of radiation scanning equipment, CBP currently scans 91 percent of the cargo and 81 percent of the passenger vehicles arriving from Canada; 97 percent of the cargo and 92 percent of the passenger vehicles arriving from Mexico, as well as 93 percent of arriving sea-borne cargo containers. To put this in perspective, just 18 months ago CBP was scanning 37 percent of arriving sea containers.

Additionally, CBP has deployed over 1,000 Radiation Isotope Identifier Devices (RIID) and over 16,000 Personal Radiation Detectors (PRD). These devices allow CBP to inspect 100 percent of all identified high-risk cargo.

Since CBP began scanning conveyances for radiation, over 195 million conveyances have been scanned, and over 1.1 million alarms have been resolved. This is a tremendous workload, and the SAFE Port Act authorized 200 new CBP Officers in each of the next 5 years to help accomplish this mission. Furthermore, the Department is currently testing the next generation of radiation detection equipment known as Advanced Spectroscopic Portals at eight locations nationwide—at Piers A and J in Long Beach, at the APM and PNCT Terminals in Newark, at the Colombia and World Trade bridges in Laredo, at the Blue Water Bridge in Port Huron, and at the Fort Street crossing in Detroit. Future deployments of ASPs, pending Secretarial certification, will allow CBP to quickly differentiate between benign materials such as kitty litter or granite, while determining which shipments pose a true risk. This perfectly supports CBP's twin goals of increasing security while facilitating the flow of legitimate trade and people.

In addition to the deployment of radiation detection equipment, CBP continues to deploy large scale imaging systems and has deployed 195 large-scale gamma ray or x-ray imaging systems nationwide. NII technology serves as a force multiplier that allows officers to detect possible anomalies between the contents of the container and the manifest. In fact, well over 5.5 million scans using NII systems were conducted in FY07.

Automated Targeting System (ATS)

CBP requires advanced electronic cargo information as mandated in the Trade Act of 2002 (including the 24-hour rule for maritime cargo). Advanced cargo information on all inbound shipments for all modes of transportation is effectively evaluated using the Automated Targeting System (ATS) before arrival in the United States. The SAFE Port Act requires CBP to seek additional data elements for ATS as well as to evaluate the entire system. CBP is complying with both these mandates.

As a matter of background, ATS provides decision-support functionality for CBP officers working in Advanced Targeting Units (ATUs) at United States ports of entry and CSI foreign ports. The system provides uniform review of cargo shipments for identification of the highest risk shipments, and presents data in a comprehensive, flexible format to address specific intelligence threats and trends. ATS uses a rules-based program to highlight potential risk, patterns, and targets. Through rules, the ATS alerts the user to data that meets or exceeds certain predefined criteria. National targeting rule sets have been implemented in ATS to provide threshold targeting for national security risks for all modes: sea, truck, rail, and air.

Working actively with the trade through the Departmental Advisory Committee on Commercial Operations (COAC), CBP has developed a new Security Filing in an effort to obtain additional advanced cargo information and enhance their ability to perform risk-based assessments prior to cargo being laden on a vessel overseas. The CBP proposal, better known as "10 plus 2" covers the following key areas:

- Ten unique data elements from importers not currently provided to CBP 24 hours prior to the foreign loading of cargo;
- Two additional data elements provided by the carriers including the Vessel Stow Plan, which is currently utilized by the vessel industry to load and discharge containers, and the Container Status Messaging, which is currently utilized by the vessel industry to track the location of containers and provide status notifications to shippers, consignees, and other related parties.

A Notice of Proposed Rulemaking (NPRM) is currently being developed. Obtaining additional information earlier in the process will increase the transparency of the global supply chain enabling the refinement of CBP's targeting processes and will provide additional information to make a more fully informed decision with respect to the risk of individual shipments.

In addition to Security Filing, CBP continually monitors the performance of weight sets and uses data analysis to modify rules and weight sets in ATS. Since 2004, ATS has undergone independent audits from the GAO and the IG. Furthermore, CBP regularly reevaluates to improve the data sets in ATS. The Office of Field Operations National Targeting and Security (NTS) office and the Office of Information Technology Targeting and Analysis Systems Program Office (TASPO) have been working together to enhance the ATS Maritime rule set capabilities for ocean cargo targeting. Under the direction of the office of field operations (OFO), TASPO placed the updated rule sets into production on March 21, 2007, to conduct initial assessments. Since that time, OFO subject matter experts and members of the Maritime Targeting Working Group have provided feedback to NTS, which re-

sulted in further refinements and enhancements to the maritime rule set. Currently NTS is modeling several versions of the new Country of Interest list to include iterations of different scores and scenarios to include entity concepts such as first time, unknown, and high volume. OFO is currently using the updated rule set for maritime threshold targeting.

Customs-Trade Partnership Against Terrorism (C–TPAT)

Customs-Trade Partnership Against Terrorism (C–TPAT) is an integral part of the CBP multi-layered strategy. CBP works in partnership with the trade community to better secure goods moving through the international supply chain. C–TPAT has enabled CBP to leverage supply chain security overseas where CBP has no regulatory reach. Throughout 2007, CBP has continued to expand and strengthen the C–TPAT program and ensure that certified member companies are fulfilling their commitment to the program by securing their goods moving across the international supply chain to the United States. To carry-out this critical tenet of C–TPAT, teams of Supply Chain Security Specialists (SCSS) will conduct validations and begin revalidations of C–TPAT members' supply chains to ensure security protocols are reliable, accurate, and effective.

The SAFE Port Act not only legislatively recognized C–TPAT, but the Act also added greater accountability by mandating that certain program activities be completed within specific time-frames, and that greater program oversight be developed for the program. CBP began implementing such changes, which were first outlined in GAO reports from 2003 and 2004, eighteen months prior to the passage of the Act and continues to make progress in this regard.

Specifically, clearly defined minimum security criteria have been developed and implemented for the major enrollment sectors and will be completed for all current enrollment sectors by this fall. The SAFE Port Act requires CBP to work with the COAC to review and modify as appropriate these criteria on an annual basis, and they have done so. This program enhancement will be completed each year as part of the development of the C–TPAT annual plan, another SAFE Port Act requirement. CBP is finalizing revisions to the C-TPAT Strategic Plan, which was first published in December 2004.

The SAFE Port Act also required CBP to review their certification processes for new members and make adjustments to strengthen this initial review if necessary. CBP has done so, and all new applications are being reviewed within 90 days.

Additionally, the Act requires that all new certified members undergo their initial validation within 1 year of acceptance into the program and be revalidated every 4 years. In 2007, CBP's goal is to complete 3,000 validations. As a point of reference, CBP completed 133 validations in 2003; 287 in 2004; 1,080 in 2005; and 2,398 in 2006. This is real progress, and it has been made possible by adding Supply Chain Security Specialists to the program.

With current staffing levels, the C–TPAT program should fulfill its operational goals for both the 2007 and 2008 calendar years. With the projected level of validations and revalidations needed to be in compliance with the Act set at just less than 3,000 per year, the current staff of 150 SCSS's should be able to manage this workload. The SAFE Port Act mandates that all revalidations must occur within 4 years of the initial validation, while the FY07 DHS Appropriations Act called for revalidations to occur within 3 years of the initial validation. Thus, the C–TPAT program is moving forward on a 3 year revalidation model to ensure compliance.

Projected revalidations alone will reach over 2,300 in 2009. The addition of Mexican Highway Carrier validations (done annually due to higher risk models) will add approximately 400. Further, required initial validations within 1 year of certification are being projected at 1,800. As a result, the final validation/revalidation totals needed would well exceed 4,000 for 2009 creating compliance issues with the current staffing numbers.

However, an additional staffing of 50 SCSS's will be brought on board with the creation of two new offices, one in Buffalo, NY, to focus principally on Canadian membership, and an office in Houston, TX, to focus on Mexican enrollment. With the addition of this staff, expected by early calendar year 2008, the C–TPAT would again see compliance with SAFE Port Act mandated timelines.

Working with COAC, CBP has also developed and implemented a pilot program using third parties to validate supply chains where CBP currently lacks full access. In May 2007, CBP selected 11 firms to act as validators in China as the Chinese government continues to deny access to CBP personnel wishing to conduct supply chain security validations. The Chinese Government has officially indicated that the matter is under review within their government, noting initially that the private sector in China may be reluctant to have C–TPAT validations conducted in-country. In an effort to show there was trade support for the process, CBP identified a cer-

tified C–TPAT partner that has significant business in China to demonstrate their willingness to participate in the validation process. Additionally, the CBP Commissioner and senior managers have traveled to China to discuss this matter with their counterparts in an effort to clarify the validation process as well as to offer a joint validation pilot involving five currently certified C–TPAT companies willing to participate. We have received no official response to this proposed project as of this date.

Interest in the pilot program has thus far been minimal. Of the more than three hundred (300) C–TPAT importers that were invited to participate in this voluntary pilot in June, less than a dozen importers have opted to do so to date. The primary concerns expressed by C–TPAT members for not participating lie in the sharing of proprietary business and security data with a third party and with the costs associated with the validation, which, as outlined in the SAFE Port Act, must be incurred by the C–TPAT member.

Container Security Standards and Procedures

CBP strongly supports and continues to seek opportunities to enhance supply chain security efforts, including enhancements to the security of the container. Indeed, securing the container is a critical part of a multi-layered approach to supply chain security. However, in order to establish minimum standards for container security, it is first necessary to ensure that there are available solutions that would significantly improve container security without significantly disrupting the flow of legitimate commerce. It should be noted that minimum security criteria for participants in the C–TPAT program do include a requirement that all C–TPAT importers must affix a high security seal to all loaded containers bound for the United States. These seals must meet or exceed the current ISO/PAS 17712 specifications for high security seals. C–TPAT membership currently accounts for 46 percent of total importations into the U.S.

Any technological solution would also need to be adopted as part of a broader supply chain security program. While CBP does not believe that, at the present time, the necessary technology exists for such solutions, CBP is working closely with the Department and is actively working with industry to test different technologies and methodologies that would provide economically and operationally viable enhancements to container security.

In-Bonds

The SAFE Port Act also required CBP to submit a report on in-bond cargo no later than June 30, 2007. CBP apologizes for the lateness of this report, which is still undergoing review, and expects to have the report issued shortly.

The final report includes a plan for closing in-bond entries at the port of arrival; an assessment of the personnel required to ensure 100 percent reconciliation of in-bond entries between the port of arrival and the port of destination or exportation; an assessment of the status of investigations of overdue in-bond shipments and an evaluation of the resources required to ensure adequate investigation of overdue in-bond shipments; a plan for tracking in-bond cargo within the Automated Commercial Environment (ACE); an assessment of whether any particular technologies should be required in the transport of in-bond cargo; an assessment of whether ports of arrival should require any additional information regarding shipments of in-bond cargo; an evaluation of the criteria for targeting and examining in-bond cargo; and an assessment of the feasibility of reducing the transit time for in-bond shipments, including an assessment of the impact of such a change on domestic and international trade. In addition, CBP is in the process of utilizing the evaluation of in-bond criteria to assist in the creation of a weight set for use in ATS to further assist in the identification of potential in-bond diversion cargo shipments.

CBP believes that the report is responsive to the concerns expressed by Congress, and a dedicated working group of experts has just concluded an in-depth review of the in-bond process and their recommendations will also address the report topics.

Office of International Trade

The mandates of the SAFE Port Act and the actions of CBP intersected again when CBP formed the Office of International Trade in October 2006. The establishment of this office serves to strengthen CBP's ability to carry out our mission of facilitating the flow of legitimate trade across U.S. borders while securing the borders and protecting the American economy from unfair trade practices and illicit commercial enterprises. The Office of International Trade consolidates trade policy, program development, and compliance measurement functions into a single office, providing greater consistency within CBP with respect to its international trade programs and operations. In addition, CBP's close working relationship with the trade community, a hallmark of CBP's operations and programs, has been further en-

hanced. The new Office of International Trade is providing CBP and the Trade community with an organization that can effectively address the growing volume and complexities of international trade and is enabling us to successfully meet the challenges inherent in managing the balance of trade and security.

In June 2007, to meet the Congressional requirements of the SAFE Port Act, CBP provided to Congress a resource optimization model (the "model") for the commercial operations and revenue function. The objectives of the model are to: (1) optimally align the workforce to achieve management performance outcomes and goals; (2) adequately address risks inherent in the priority trade issues; and (3) comply with statutory requirements. The model has been designed to determine the right number and right mix of resources to facilitate legitimate trade while enforcing the trade laws.

Additionally, in preparation of submitting a report on the reorganization into the Office of International Trade, CBP has been meeting regularly with the COAC subcommittee on the Office of International Trade. During this first year, the subcommittee has been working together to find mutually beneficially process improvements to facilitate legitimate trade, which in turn will assist CBP in its trade enforcement efforts.

Conclusion

The steps that CBP is taking to implement the SAFE Port Act are and will be an extremely important aspect to the security of the Nation. Through the SAFE Port Act, Congress has recognized and bolstered many of our aggressive programs to enhance security while assuring the facilitation of legitimate trade. We appreciate the close cooperative relationship the Department of Homeland Security and CBP had with the House and Senate in the development of the Act, and we look forward to the continued interaction to promote our mission and ensure the safety of American citizens and commerce.

Senator LAUTENBERG. Thank you very much. And now, Mr. Caldwell?

STATEMENT OF STEPHEN L. CALDWELL, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. CALDWELL. Good morning, Senator Lautenberg, Senator Stevens and Senator Lott. Thank you very much for inviting me here today to talk about port security. By passing the SAFE Port Act one year ago, Congress basically approved the things agencies were doing but just wanted the things done better and faster. Given the wide scope of the SAFE Port Act and the details already provided in my statement and by the other witnesses, I'm going to focus my oral comments on the five areas where GAO is doing evaluations for this Committee.

This work can be divided into two broad areas: Coast Guard work and Customs work. Let me start out with the Coast Guard work.

Regarding port security operations, the Coast Guard, to its credit, has developed measurable requirements for its activities at the ports. These are activities such as boarding suspicious ships, escorting selected vessels, enforcing security zones and patrolling harbors. These requirements, part of the Coast Guard's Operation Neptune Shield, are scalable and can be increased as the MARSEC level increases.

To meet these requirements with the limited resources the Coast Guard has, they have developed a strategy to selectively adjust some of their requirements, partner with State and local agencies, and analyze their resource needs constantly. Unfortunately, even with these strategies, some Coast Guard sectors are still having

difficulties meeting their security requirements over a prolonged period of time.

Regarding facilities—thousands of MTSA-regulated facilities have developed security plans. The Coast Guard has generally approved these plans and inspected these facilities once a year to ensure their compliance. However, the SAFE Port Act requires the Coast Guard to complete such inspections twice a year and to include at least one unannounced inspection.

The Coast Guard faces three challenges as they ramp up inspections to meet this new requirement. First, the current method of conducting unannounced inspections varies considerably by sector so the Coast Guard is currently in the process to issue clear guidance on what constitutes an unannounced or spot check. Second, while the Coast Guard has trained hundreds of inspectors, many of these inspectors have now rotated to other positions and with the increased requirements, the Coast Guard is going to have to figure out exactly how many inspectors they're going to need, how to get them trained and get them in the right sectors. And then third, the Coast Guard needs to improve the current data that it keeps on inspections (that data is currently flawed) and then conduct some analysis of that data to better manage the program.

Regarding inspection of foreign ports, the Coast Guard has a program in place to visit them and to evaluate their compliance with international security standards. The Coast Guard has currently visited about 109 of the 140 ports. The SAFE Port Act went on to require that each country be revisited within 3 years, creating a challenge for the Coast Guard to replace its current cadre of experienced inspectors with new ones needed to meet these new timelines.

The Coast Guard faces other challenges in this program as well. The visits are set up through the sovereign host nation, which places some limitations on the Coast Guard in terms of where to visit and the scope of their visits. And even if this was not an issue, it's hard to assess maritime security for an entire country by relatively short visits to a select number of ports. In addition, some of the countries that are visited and have security problems are poor countries in Africa or the Caribbean, which lack the resources to fund and/or sustain needed improvements to port security.

Now, I'll turn to the Customs programs to improve container security. We've reported twice on the CSI program and CBP has made continued progress in better managing that program. Similarly, we've reviewed the C–TPAT program twice and again, we've seen several improvements in the management of the program. We'll have full reports on both of those programs to the Committee later this year.

One indication of the success for both CSI and C–TPAT, is that international organizations and other countries are currently in the process of adopting security regimes very similar to these two CBP programs.

The biggest challenge ahead for CBP has to do with the 100 percent scanning requirement that was in the 9/11 Act. While we have not done a detailed review of the 100 percent scanning requirement, the topic has come up repeatedly when we meet with various foreign officials and international organizations and we have vis-

ited two of the SFI pilot ports. Based on this preliminary work, we have identified a number of challenges, which are detailed in my written statement.

Looking ahead, we will continue working with the agencies and with the Congress and this Committee to help you with oversight to keep our ports as secure as practical. Thank you very much.

[The prepared statement of Mr. Caldwell follows:]

PREPARED STATEMENT OF STEPHEN L. CALDWELL, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss port and cargo security functions related to provisions of the Security and Accountability for Every Port Act (SAFE Port Act).[1] The Nation's 361 seaports are the gateway for more than 80 percent of our foreign trade. Worldwide, some 30 large ports, spread across North America, Asia, and Europe constitute the world's primary, interdependent trading web. Much of this trade—particularly high-value cargo—enters and leaves in cargo containers.

In our post-9/11 environment, however, the potential security weaknesses presented by these economic gateways have become apparent. Sprawling, easily accessible by water and land, often close to urban areas, and containing facilities that represent opportunities for inflicting significant damage as well as causing economic mayhem, ports present potential terrorist targets. Further, they are potential conduits for weapons prepared elsewhere and concealed in cargo designed to move quickly to many locations beyond the ports themselves.

Since the 9/11 attacks, Congress has established a new port security framework—much of which was set in place by the Maritime Transportation Security Act (MTSA)[2]. Enacted in November 2002, MTSA was designed, in part, to help protect the Nation's ports and waterways from terrorist attacks by requiring a wide range of security improvements. Among the major requirements included in MTSA were (1) conducting vulnerability assessments for port facilities and vessels; (2) developing security plans to mitigate identified risks for the national maritime system, ports, port facilities, and vessels; (3) developing the Transportation Worker Identification Credential (TWIC), a biometric identification card to help restrict access to secure areas to only authorized personnel; and (4) establishing of a process to assess foreign ports, from which vessels depart on voyages to the United States. The Department of Homeland Security (DHS)—itself a creation of the new security environment brought on by the 9/11 attacks—administers much of this framework, which also attempts to balance security priorities with the need to facilitate legitimate trade.

The SAFE Port Act, which was enacted in October 2006, is one of the latest additions to this port security framework. The Act made a number of adjustments to programs within this framework, creating additional programs or lines of effort and altering others. The SAFE Port Act created and codified new programs and initiatives, and amended some of the original provisions of MTSA. The SAFE Port Act included provisions that: (1) codified the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C–TPAT), two programs administered by Customs and Border Protection (CBP) to help reduce threats associated with cargo shipped in containers; (2) required interagency operational centers where agencies organize to fit the security needs of the port area at selected ports; (3) set an implementation schedule and fee restrictions for TWIC; (4) required that all containers entering high volume U.S. ports be scanned for radiation sources by December 31, 2007; and (5) required additional data be made available to CBP for targeting cargo containers for inspection.[3] This statement summarizes our recently completed and ongoing work for this Committee on these areas.

Over the past several years, we have examined and reported on many of the programs in this new port security framework. This statement is designed both to provide an overview of what we have earlier reported about these programs and to describe, with the preliminary information available, what DHS is doing as a result of the SAFE Port Act requirements and the challenges the agency faces in doing so. This statement discusses three key areas and 18 programs, as shown in Table 1.

Table 1: Summary of Three Key Areas and 18 Programs in This Statement

Program	Description
Overall Port Security	
Area Maritime Security Committees	Committees consisting of key port stakeholders who share information and develop port security plans.
Interagency Operational Centers	Command centers where agencies share information, coordinate their activities, and coordinate joint efforts.
Port security operations	Activities to maintain security and deter attacks, such as boat patrols and vessel escorts.
Area Maritime Security Plans	Plan laying out local port vulnerabilities, responsibilities, and some response actions.
Port security exercises	Exercises among various port stakeholders to test the effectiveness of port security plans.
Evaluations of security at foreign ports	Coast Guard program where officers visit and assess security conditions at foreign ports.
Port Facility Security	
Port facility security plans	Plans that include, among other things, operational and physical security measures and procedures for responding to security threats.
Port facility security compliance monitoring	Coast Guard reviews of port facility security plans and their compliance with such plans.
Transportation Worker Identification Credential	Biometric identification cards to be issued to port workers to help secure access to areas of ports.
Background checks	DHS requirements for persons who enter secure or restricted areas or transport hazardous cargo.
Container Security	
Automated Targeting System	Risk-based decision system to determine cargo shipped in containers requiring inspection.
Customs In-Bond System	The in-bond system allows goods to transit the United States without officially entering U.S. commerce.
Container Security Initiative	Stationing CBP officers at foreign ports to help identify and inspect high-risk cargo to be shipped in containers destined for the United States.
Customs-Trade Partnership Against Terrorism	Partnership between private companies and CBP to improve international supply chain security.
Promoting Global Standards	Efforts to work with members of the customs and trade community on approaches to standardizing supply chain security.
Megaports Initiative	Radiation detection technology at foreign ports to stop the proliferation of weapons of mass destruction.
Secure Freight Initiative	Combines Container Security Initiative scanning with Megaports Initiative radiation detection at foreign ports.
100 Percent Container Scanning at Foreign Ports	Scanning by nonintrusive imaging and radiation detection equipment of all cargo containers at foreign ports inbound to the United States by 2012, with possible exceptions.

Source: GAO.

This statement is organized into three main areas, as follows:

- programs related to overall port security, such as those for coordinating among stakeholders, conducting security operations, developing security plans, and conducting exercises to test security procedures;
- programs related specifically to security at individual facilities, such as examining security measures and ensuring that only properly cleared individuals have access to port areas; and,
- programs related specifically to the international supply chain and to cargo container security, such as screening containers at ports both here and abroad and forming partnerships with the private sector.

This statement is based primarily on a body of work we completed in response to Congressional requests and mandates for analysis of maritime, port, and cargo

security efforts of the Federal Government.[4] In some cases, we provide preliminary observations from our ongoing work. Thus, the timeliness of the data that were the basis for our prior reporting varies depending on when our products were issued and the preliminary observations are subject to change as we complete our work.

We conducted all of our work in accordance with generally accepted government auditing standards. To perform both our completed and ongoing work we visited several domestic and overseas ports; reviewed agency program documents, port security plans, and post-exercise reports, and other documents; and interviewed officials from the Federal, state, local, private, and international sectors. The officials were from a wide variety of port stakeholders to include Coast Guard, CBP, TSA, port authorities, terminal operators, vessel operators, foreign governments, and international organizations. While this body of work does not cover all the provisions of the SAFE Port Act, it does cover a wide range of these provisions as shown in Table 1.

We provided a draft of this testimony to DHS agencies and incorporated technical comments as appropriate.

Summary

Regarding overall security at U.S. ports, Federal agencies have taken a number of steps to improve maritime security and implement many aspects of MTSA. The Coast Guard has established Area Maritime Security Committees (AMSCs) to coordinate activities and share information among the various stakeholders at specific ports. The Coast Guard also has local operations centers where it coordinates its activities. The SAFE Port Act requires that all high-priority ports have interagency operational centers.[5] Given the capabilities and organization of its existing centers, the Coast Guard estimates it will cost $260 million to meet this requirement. The Coast Guard also conducts a number of operations at U.S. ports to deter and prevent terrorist attacks, such as harbor patrols or vessel escorts. While the Coast Guard has set specific requirements for the level of these activities, they are not always able to complete them at some ports due to resource constraints. The Coast Guard, in collaboration with the MTSA-required AMSCs, has written port-specific security plans to deter and respond to terrorist attacks—but these plans do not fully address recovery issues (*e.g.,* how to reopen a port after an attack) and natural disasters (*e.g.,* hurricanes or earthquakes). The Coast Guard, again in collaboration with the AMSCs, has sponsored exercises to test the port security plans. But the Coast Guard will face challenges expanding the program in line with SAFE Port Act requirements to include new scenarios and improve the communication of lessons learned during exercises. Finally, security in our own ports is dependent on security in foreign ports where vessels depart for the United States. The Coast Guard has implemented a MTSA-required program to work with foreign countries to inspect and strengthen security at their ports, but will likely face challenges in hiring and training sufficient staff to meet SAFE Port Act requirements to increase the frequency of such inspections. A related challenge is that many of the foreign countries that the Coast Guard has visited—to include several countries in the Caribbean Basin—are poor and lack the resources to make major improvements on their own.

Regarding security at approximately 3,000 individual facilities, again Federal agencies and the facilities themselves have taken positive steps. In line with MTSA, facilities have written and implemented security plans and the Coast Guard has generally inspected such facilities to verify compliance and take enforcement actions where necessary. The SAFE Port Act increased the scope and frequency of these activities, doubling the frequency of Coast Guard inspections of facilities and requiring unannounced inspections. The Coast Guard told us that it is likely to face challenges in putting enough trained inspectors in place to meet the additional workload, especially since many experienced inspectors are scheduled to rotate to other duties. To control access to individual facilities at ports, MTSA required a program to develop secure and biometric Transportation Worker Identification Credentials (TWIC). Under the program, transportation workers would have to undergo background checks to receive TWIC cards. The SAFE Port Act established a July 1, 2007 milestone for the implementation of the TWIC program at the 10 highest risk ports. The Transportation Security Administration (TSA), the agency responsible for implementing TWIC, did not meet the July deadline, citing the need to conduct additional testing of the systems and technologies that will be used to enroll the estimated 770,000 workers that are required to obtain a TWIC card. Finally, while DHS has created the Screening Coordination Office (SCO) to better coordinate TWIC with other programs that require background checks, it will be challenged to fully coordinate all the DHS screening programs, ensuring that the cost and benefits of potentially eliminating or keeping different screening programs are properly considered, and coordinating with other Federal screening programs outside DHS.

Regarding the security of cargo containers—which carry a large volume of the world's commerce through our ports—CBP has developed a layered security strategy to identify and inspect containers that may contain terrorist weapons of mass destruction. CBP has refined its Automated Targeting System (ATS) to better analyze shipping information and identify suspicious containers, though it does not have the most up to date information for certain containers—that transit beyond the ports as part of the in-bond system, which allows goods to transit the United States without officially entering U.S. commerce. CBP has expanded and improved the management of its Container Security Initiative (CSI) where the agency places U.S. customs officials in foreign ports to help target and inspect suspicious containers. Similarly, CBP has expanded and improved the management of its Customs-Trade Partnership Against Terrorism (C–TPAT) where private companies agree to improve the security of their supply chains in exchange for reduced scrutiny over their shipments. The SAFE Port Act codified these two programs into law and required enhanced management and oversight of these programs. CBP is working to meet these new requirements, but our prior and ongoing work suggest that it may face challenges setting equipment standards and conducting validations of company practices. The Department of Energy (DOE) is expanding its Megaports program that complements CSI by providing foreign nations with radiation detection equipment to scan containers moving through their ports. The SAFE Port Act also required pilot programs to test new technologies or combine existing technologies to test the feasibility of scanning all U.S.-bound containers overseas. More recent legislation required that all containers bound for the United States be scanned overseas by 2012 with possible extensions for individual ports. Our preliminary observations suggest this requirement potentially creates new challenges for CBP in terms of integrating this with existing programs, working with foreign governments, overcoming logistical barriers, testing new technology, determining resource requirements and responsibilities, and other issues.

We have reviewed many of the MTSA and SAFE Port Act related programs and made prior recommendations to the appropriate agencies to develop strategic plans, better plan their use of human capital, establish performance measures, and otherwise improve the operations of these programs. In general, these agencies have concurred with our recommendations and are making progress implementing them.

Prior Actions Have Improved Port Security, but Issues Remain

Port security overall has improved because of the development of organizations and programs such as AMSCs, Area Maritime Security Plans (area plans), maritime security exercises, and the International Port Security Program, but challenges to successful implementation of these efforts remain. Additionally, agencies may face challenges addressing the additional requirements directed by the SAFE Port Act, such as a provision that DHS establish interagency operational centers at all high-risk priority ports. AMSCs and the Coast Guard's sector command centers have improved information sharing, but the types and ways information is shared varies.[6] Area plans, limited to security incidents, could benefit from unified planning to include an all-hazards approach. Maritime security exercises would benefit from timely and complete after action reports, increased collaboration across Federal agencies, and broader port level coordination. The Coast Guard's International Port Security Program is currently evaluating the antiterrorism measures maintained at foreign seaports.

Area Maritime Security Committees Share Information and Coast Guard Expands Interagency Operational Centers

Two main types of forums have developed for agencies to coordinate and share information about port security: area committees and Coast Guard sector command centers. AMSCs serve as a forum for port stakeholders, facilitating the dissemination of information through regularly scheduled meetings, issuance of electronic bulletins, and sharing key documents. MTSA provided the Coast Guard with the authority to create AMSCs—composed of Federal, state, local, and industry members—that help to develop the area plan for the port. As of August 2007, the Coast Guard had organized 46 AMSCs. As part of an ongoing effort to improve its awareness of the maritime domain, the Coast Guard developed 35 sector command centers, four of which operate in partnership with the U.S. Navy.[7] Each has flexibility to assemble and operate in a way that reflects the needs of its port area, resulting in variations in the number of participants, the types of state and local organizations involved, and the way in which information is shared. Some examples of information shared includes assessments of vulnerabilities at specific port locations, information about potential threats or suspicious activities, and Coast Guard strategies intended for use in protecting key infrastructure.

We have previously reported that both of these types of forums have helped foster cooperation and information-sharing.[8] We further reported that AMSCs provided a structure to improve the timeliness, completeness, and usefulness of information sharing between Federal and nonFederal stakeholders. These committees improved upon previous information-sharing efforts because they established a formal structure and new procedures for sharing information. In contrast to AMSCs, the Coast Guard's sector command centers can provide continuous information about maritime activities and involve various agencies directly in operational decisions using this information. We have reported that these centers have improved information sharing, and the types of information and the way information is shared varies at these centers depending on their purpose and mission, leadership and organization, membership, technology, and resources.

The SAFE Port Act called for establishment of interagency operational centers, directing the Secretary of DHS to establish such centers at all high-priority ports no later than 3 years after the Act's enactment. The Act required that the centers include a wide range of agencies and stakeholders and carry out specified maritime security functions. In addition to authorizing the appropriation of funds and requiring DHS to provide the Congress a proposed budget and cost-sharing analysis for establishing the centers, the Act directed the new interagency operational centers to utilize the same compositional and operational characteristics of existing sector command centers. According to the Coast Guard, none of the 35 centers meets the requirements set forth in the SAFE Port Act. Nevertheless, the four centers the Coast Guard operates in partnership with the Navy are a significant step in meeting these requirements, according to a senior Coast Guard official. The Coast Guard is currently piloting various aspects of future interagency operational centers at existing centers and is also working with multiple interagency partners to further develop this project.[9] DHS has submitted the required budget and cost-sharing analysis proposal, which outlines a 5-year plan for upgrading its centers into future interagency operations centers to continue to foster information sharing and coordination in the maritime domain. The Coast Guard estimates the total acquisition cost of upgrading 24 sectors that encompass the Nation's high priority ports into interagency operations centers will be approximately $260 million, to include investments in information system, sensor network, facilities upgrades and expansions. According to the Coast Guard, future interagency operations centers will allow the Coast Guard and its partners to use port surveillance with joined tactical and intelligence information, and share this data with port partners working side by side in expanded facilities.

In our April 2007 testimony, we reported on various challenges the Coast Guard faces in its information sharing efforts.[10] These challenges include obtaining security clearances for port security stakeholders and creating effective working relationships with clearly defined roles and responsibilities. In our past work, we found the lack of Federal security clearances among area committee members had been routinely cited as a barrier to information sharing.[11] In turn, this inability to share classified information may limit the ability to deter, prevent, and respond to a potential terrorist attack. The Coast Guard, having lead responsibility in coordinating maritime information, has made improvements to its program for granting clearances to area committee members and additional clearances have been granted to members with a need to know as a result.[12] In addition, the SAFE Port Act includes a specific provision requiring DHS to sponsor and expedite security clearances for participants in interagency operational centers. However, the extent to which these efforts will ultimately improve information sharing is not yet known. As the Coast Guard expands its relationships with multiple interagency partners, collaborating and sharing information effectively under new structures and procedures will be important. While some of the existing centers achieved results with existing interagency relationships, other high-priority ports might face challenges establishing new working relationships among port stakeholders and implementing their own interagency operational centers. Finally, addressing potential overlapping responsibilities—such as leadership roles for the Coast Guard and its interagency partners—will be important to ensure that actions across the various agencies are clear and coordinated.

Operations to Provide Overall Port Security Face Resource Constraints

As part of its operations, the Coast Guard has also imposed additional activities to provide overall port security. The Coast Guard's operations order, Operation Neptune Shield, first released in 2003, specifies the level of security activities to be conducted. The order sets specific activities for each port; however, the amount of each activity is established based on the port's specific security concerns. Some examples of security activities include conducting waterborne security patrols, boarding high-

interest vessels, escorting vessels into ports, and enforcing fixed security zones. When a port security level increases, the amount of activity the Coast Guard must conduct also increases.[13] The Coast Guard uses monthly field unit reports to indicate how many of its security activities it is able to perform. Our review of these field unit reports indicates that many ports are having difficulty meeting their port security responsibilities, with resource constraints being a major factor. In an effort to meet more of its security requirements, the Coast Guard uses a strategy that includes partnering with other government agencies, adjusting its activity requirements, and acquiring resources. Despite these efforts, many ports are still having difficulty meeting their port security requirements. The Coast Guard is currently studying what resources are needed to meet certain aspects of its port security program, but to enhance the effectiveness of its port security operations, a more comprehensive study to determine all additional resources and changes to strategy to meet minimum security requirements may be needed. We will be issuing a report on this issue in the near future.

Area Plans Are in Place but Need to Address Recovery and Natural Disasters

Area plans—another MTSA requirement—and their specific provisions have been specified by regulation and Coast Guard directive. Implementing regulations for MTSA specified that area plans include, among other things, operational and physical security measures in place at the port under different security levels, details of the security incident command and response structure, procedures for responding to security threats including provisions for maintaining operations in the port, and procedures to facilitate the recovery of the marine transportation system after a security incident. A Coast Guard Navigation and Vessel Inspection Circular (NVIC) provided a common template for area plans and specified the responsibilities of port stakeholders under them.[14] As of September 2007, 46 area plans are in place at ports around the country. The Coast Guard approved the plans by June 1, 2004, and MTSA requires that they be updated at least every 5 years.

The SAFE Port Act added a requirement to area plans, which specified that they include recovery issues by identifying salvage equipment able to restore operational trade capacity. This requirement was established to ensure that the waterways are cleared and the flow of commerce through United States ports is reestablished as efficiently and quickly as possible after a security incident. While the Coast Guard sets out the general priorities for recovery operations in its guidelines for the development of area plans, we have found that this guidance offers limited instruction and assistance for developing procedures to address recovery situations.

The Maritime Infrastructure Recovery Plan (MIRP) recognizes the limited nature of the Coast Guard's guidance and notes the need to further develop recovery aspects of the area plans.[15] The MIRP provides specific recommendations for developing the recovery sections of the area plans. The area plans that we reviewed often lacked recovery specifics and none had been updated to reflect the recommendations made in the MIRP. The Coast Guard is currently updating the guidance for the area plans and aims to complete the updates by the end of calendar year 2007 so that the guidance will be ready for the mandatory 5-year re-approval of the area plans in 2009. Coast Guard officials commented that any changes to the recovery section would need to be consistent with the national protocols developed for the SAFE Port Act.[16] Additionally, related to recovery planning, the Coast Guard and CBP have developed specific interagency actions focused on response and recovery. This should provide the Coast Guard and CBP with immediate security options for the recovery of ports and commerce.

Further, area plans generally do not address natural disasters (*i.e.,* they do not have an all-hazards approach).[17] In a March 2007 report examining how ports are dealing with planning for natural disasters such as hurricanes and earthquakes, we noted that area plans cover security issues but not other issues that could have a major impact on a port's ability to support maritime commerce.[18] As currently written, area plans are concerned with deterring and, to a lesser extent, responding to security incidents. We found, however, that unified consideration of all risks—natural and man-made—faced by a port may be beneficial. Because of the similarities between the consequences of terrorist attacks and natural or accidental disasters, much of the planning for protection, response, and recovery capabilities is similar across all emergency events. Combining terrorism and other threats can thus enhance the efficiency of port planning efforts. This approach also allows port stakeholders to estimate the relative value of different mitigation alternatives. The exclusion of certain risks from consideration, or the separate consideration of a particular type of risk, raises the possibility that risks will not be accurately assessed or compared, and that too many or too few resources will be allocated toward mitigation of a particular risk.

As ports continue to revise and improve their planning efforts, available evidence indicates that by taking a systemwide approach and thinking strategically about using resources to mitigate and recover from all forms of disaster, ports will be able to achieve the most effective results. Area plans provide a useful foundation for establishing an all-hazards approach. While the SAFE Port Act does not call for expanding area plans in this manner, it does contain a requirement that natural disasters and other emergencies be included in the scenarios to be tested in the Port Security Exercise Program. On the basis of our prior work, we found there are challenges in using area committees and plans as the basis for broader all-hazards planning. These challenges include determining the extent that security plans can serve all-hazards purposes. We recommended that DHS encourage port stakeholders to use the existing security-oriented area committees and MTSA-required area plans to discuss all-hazards planning. DHS concurred with this recommendation.

Maritime Security Exercises Require a Broader Scope and Participation

The Coast Guard Captain of the Port and the area committee are required by MTSA regulations to conduct or participate in exercises to test the effectiveness of area plans annually, with no more than 18 months between exercises. These exercises—which have been conducted for the past several years—are designed to continuously improve preparedness by validating information and procedures in the area plan, identifying weaknesses and strengths, and practicing command and control within an incident command/unified command framework. In August 2005, the Coast Guard and the TSA initiated the Port Security Training Exercise Program (PortSTEP)—an exercise program designed to involve the entire port community, including public governmental agencies and private industry, and intended to improve connectivity of various surface transportation modes and enhance area plans. Between August 2005 and October 2007, the Coast Guard expected to conduct PortSTEP exercises for 40 area committees and other port stakeholders. Additionally, the Coast Guard initiated its own Area Maritime Security Training and Exercise Program (AMStep) in October 2005. This program was also designed to involve the entire port community in the implementation of the Area Maritime Security Plan (AMSP). Between the two programs, PortSTEP and AMStep, all Area Maritime Security Committees (AMSCs) have received a port security exercise each year since inception.

The SAFE Port Act included several new requirements related to security exercises, such as establishing a Port Security Exercise Program to test and evaluate the capabilities of governments and port stakeholders to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism, natural disasters, and other emergencies at facilities that MTSA regulates. The Act also required the establishment of a port security exercise improvement plan process that would identify, disseminate, and monitor the implementation of lessons learned and best practices from port security exercises.

Though we have not specifically examined compliance with these new requirements, our work in examining past exercises suggests that implementing a successful exercise program faces several challenges.[19] These challenges include setting the scope of the program to determine how exercise requirements in the SAFE Port Act differ from area committee exercises that are currently performed. This is especially true for incorporating recovery scenarios into exercises. In this past work, we also found that Coast Guard terrorism exercises frequently focused on prevention and awareness, but often did not include recovery activities. According to the Coast Guard, with the recent emphasis on planning for recovery operations, it has held several exercises over the past year that have included in part, or solely, recovery activities. It will be important that future exercises also focus on recovery operations so public and private stakeholders can cover gaps that might hinder commerce after a port incident. Other long-standing challenges include completing after-action reports in a timely and thorough manner and ensuring that all relevant agencies participate. According to the Coast Guard, as the primary sponsor of these programs, it faces a continuing challenge in getting comprehensive participation in these exercises.

The Coast Guard Is Evaluating the Security of Foreign Ports, but Faces Resource Challenges

The security of domestic ports also depends upon security at foreign ports where cargoes bound for the United States originate. To help secure the overseas supply chain, MTSA required the Coast Guard to develop a program to assess security measures in foreign ports and, among other things, recommend steps necessary to improve security measures in those ports. The Coast Guard established this program, called the International Port Security Program, in April 2004. Under this pro-

gram, the Coast Guard and host nations review the implementation of security measures in the host nations' ports against established security standards, such as the International Maritime Organization's International Ship and Port Facility Security (ISPS) Code.[20] Coast Guard teams have been established to conduct country visits, discuss security measures implemented, and collect and share best practices to help ensure a comprehensive and consistent approach to maritime security in ports worldwide. The conditions of these visits, such as timing and locations, are negotiated between the Coast Guard and the host nation. Coast Guard officials also make annual visits to the countries to obtain additional observations on the implementation of security measures and ensure deficiencies found during the country visits are addressed.[21]

Both the SAFE Port Act and other Congressional directions have called for the Coast Guard to increase the pace of its visits to foreign countries. Although MTSA did not set a time-frame for completion of these visits, the Coast Guard initially set a goal to visit the approximately 140 countries that conduct maritime trade with the United States by December 2008. In September 2006, the conference report accompanying the Fiscal Year 2007 DHS Appropriations Act directed the Coast Guard to "double the amount" at which it was conducting its visits.[22] Subsequently, in October 2006, the SAFE Port Act required the Coast Guard to reassess security measures at the foreign ports every 3 years. Coast Guard officials said they will comply with the more stringent requirements and will reassess countries on a 2-year cycle. With the expedited pace, the Coast Guard now expects to assess all countries by March 2008, after which reassessments will begin.

We are currently conducting a review of the Coast Guard's International Port Security Program that evaluates the Coast Guard's implementation of international enforcement programs. The report, expected to be issued in early 2008, will cover issues related to the program, such as the extent to which the program is using a risk-based approach in carrying out its work, what challenges the program faces as it moves forward, and the extent to which the observations collected during the country visits are used by other programs such as the Coast Guard's port state control inspections and high interest vessel boarding programs.

As of September 2007, the Coast Guard reported that it has visited 109 countries under this program and plans to visit another 29 more by March 2008.[23] For the countries for which the Coast Guard has issued a final report, the Coast Guard reported that most had "substantially implemented the security code," while a few countries were found to have not yet implemented the ISPS Code and will be subject to a reassessment or other sanctions. The Coast Guard also found several facilities needing improvements in areas such as access controls, communication devices, fencing, and lighting.

While our review is still preliminary, Coast Guard officials told us that to plan and prepare for the next cycle of reassessments that are to begin next year, they are considering modifying their current visit methodology to incorporate a risk-based approach to prioritize the order and intensity of the next round of country visits. To do this, they have consulted with a contractor to develop an updated country risk prioritization model. Under the previous model, the priority assigned to a country for a visit was weighted heavily toward the volume of U.S. trade with that country. The new model being considered is to incorporate other factors, such as corruption and terrorist activity levels within the countries. Program officials told us that the details of this revised approach have yet to be finalized.

Coast Guard officials told us that as they complete the first round of visits and move into the next phase of revisits, challenges still exist in implementing the program. One challenge identified was that the faster rate at which foreign ports will now be reassessed will require hiring and training new staff—a challenge the officials expect will be made more difficult because experienced personnel who have been with the program since its inception are being transferred to other positions as part of the Coast Guard's rotational policy. These officials will need to be replaced with newly assigned personnel.

Reluctance by some countries to allow the Coast Guard to visit their ports due to concerns over sovereignty was another challenge cited by program officials in completing the first round of visits. According to these officials, before permitting Coast Guard officials to visit their ports, some countries insisted on visiting and assessing a sample of U.S. ports. The Coast Guard was able to accommodate their request through the program's reciprocal visit feature in which the Coast Guard hosts foreign delegations to visit U.S. ports and observe ISPS Code implementation in the United States. This subsequently helped gain the cooperation of the countries in hosting a Coast Guard visit to their own ports. However, as they begin to revisit countries as part of the program's next phase, program officials stated that sovereignty concerns may still be an issue. Some countries may be reluctant to host

a comprehensive country visit on a recurring basis because they believe the frequency—once every 2 to 3 years—too high. Sovereignty also affects the conditions of the visits, such as timing and locations, because such visits are negotiated between the Coast Guard and the host nation. Thus the Coast Guard team making the visit could be precluded from seeing locations that are not in compliance.

Another challenge program officials cite is having limited ability to help countries build on or enhance their capacity to implement the ISPS Code requirements. For example, the SAFE Port Act required that GAO report on various aspects of port security in the Caribbean Basin. We earlier reported that although the Coast Guard found that most of the countries had substantially implemented the ISPS Code, some facilities needed to make improvements or take additional measures.[24] In addition, our discussions with facility operators and government officials in the region indicated that assistance—such as additional training—would help enhance their port security. Program officials stated that while their visits provide opportunities for them to identify potential areas to improve or help sustain the security measures put in place, other than sharing best practices or providing presentations on security practices, the program does not currently have the resources to directly assist countries with more in-depth training or technical assistance. To overcome this, program officials have worked with other agencies (*e.g.,* the Departments of Defense and State) and international organizations (*e.g.,* the Organization of American States) to secure funding for training and assistance to countries where port security conferences have been held (*e.g.,* the Dominican Republic and the Bahamas). Program officials indicated that as part of reexamining the approach for the program's next phase, they will also consider possibilities to improve the program's ability to provide training and capacity building to countries when a need is identified.

Port Facility Security Efforts Continue, but Additional Evaluation Is Needed

To improve the security at individual facilities at ports, many long-standing programs are underway. However, new challenges to their successful implementation have emerged. The Coast Guard is required to conduct assessments of security plans and facility compliance inspections, but faces challenges in staffing and training to meet the SAFE Port Act's additional requirements such as the sufficiency of trained personnel and guidance to conduct facility inspections. TSA's TWIC program has addressed some of its initial program challenges, but will continue to face additional challenges as the program rollout continues. Many steps have been taken to ensure that transportation workers are properly screened, but redundancies in various background checks have decreased efficiency and highlighted the need for increased coordination.

The Coast Guard's Compliance Monitoring of Maritime Facilities Identifies Deficiencies, but Program Effectiveness Overall Has Not Been Evaluated

MTSA and its implementing regulations required owners and operators of certain maritime facilities (*e.g.,* power stations, chemical manufacturing facilities, and refineries that are located on waterways and receive foreign vessels) to conduct assessments of their security vulnerabilities, develop security plans to mitigate these vulnerabilities, and implement measures called for in the security plans by July 1, 2004. Under the Coast Guard regulations, these plans are to include items such as measures for access control, responses to security threats, and drills and exercises to train staff and test the plan.[25] The plans are "performance-based," meaning that the Coast Guard has specified the outcomes it is seeking to achieve and has given facilities responsibility for identifying and delivering the measures needed to achieve these outcomes.

Under MTSA, Coast Guard guidance calls for the Coast Guard to conduct one onsite facility inspection annually to verify continued compliance with the plan. The SAFE Port Act, enacted in 2006, required the Coast Guard to conduct at least two inspections—one of which was to be unannounced—of each facility annually. We currently have ongoing work that reviews the Coast Guard's oversight strategy under MTSA and SAFE Port Act requirements. The report, expected later this year, will cover, among other things, the extent to which the Coast Guard has met its inspection requirements and found facilities to be in compliance with its security plans, the sufficiency of trained inspectors and guidance to conduct facility inspections, and aspects of the Coast Guard's overall management of its MTSA facility oversight program, particularly documenting compliance activities.

Our work is preliminary. However, according to our analysis of Coast Guard records and statements from officials, the Coast Guard seems to have conducted facility compliance exams annually at most—but not all—facilities. Redirection of staff

to a higher-priority mission, such as Hurricane Katrina emergency operations, may have accounted for some facilities not having received an annual exam. The Coast Guard also conducted a number of unannounced inspections—about 4,500 in 2006, concentrated in around 1,200 facilities—prior to the SAFE Port Act's passage. According to officials we spoke with, the Coast Guard selected facilities for unannounced inspection based on perceived risk and inspection convenience (*e.g.,* if inspectors were already at the facility for another purpose). The Coast Guard has identified facility plan compliance deficiencies in about one-third of facilities inspected each year, and the deficiencies identified are concentrated in a small number of categories (*e.g.,* failure to follow the approved plan for ensuring facility access control, recordkeeping, or meeting facility security officer requirements). We are still in the process of reviewing the data Coast Guard uses to document compliance activities and will have additional information in our forthcoming report.

Sectors we visited reported having adequate guidance and staff for conducting consistent compliance exams, but until recently, little guidance on conducting unannounced inspections, which are often incorporated into work while performing other mission tasks. Lacking guidance on unannounced inspections, the process for conducting one varied considerably in the sectors we visited. For example, inspectors in one sector found the use of a telescope effective in remotely observing facility control measures (such as security guard activities), but these inspectors primarily conduct unannounced inspections as part of vehicle patrols. Inspectors in another sector conduct unannounced inspections at night, going up to the security gate and querying personnel about their security knowledge (*e.g.,* knowledge of high-security level procedures). As we completed our fieldwork, the Coast Guard issued a Commandant message with guidance on conducting unannounced inspections. This message may provide more consistency, but how the guidance will be applied and its impact on resource needs remain uncertain. Coast Guard officials said they plan to revise their primary circular on facility oversight by February 2008. They are also planning to revise MTSA regulations to conform to SAFE Port Act requirements in 2009 (in time for the reapproval of facility security plans) but are behind schedule.

We recommended in June 2004 that the Coast Guard evaluate its compliance inspection efforts taken during the initial 6-month period after July 1, 2004, and use the results to strengthen its long-term strategy for ensuring compliance.[26] The Coast Guard agreed with this recommendation. Nevertheless, based on our ongoing work, it appears that the Coast Guard has not conducted a comprehensive evaluation of its oversight program to identify strengths or target areas for improvement after 3 years of program implementation. Our prior work across a wide range of public and private-sector organizations shows that high-performing organizations continuously assess their performance with information about results based on their activities.[27] For decisionmakers to assess program strategies, guidance, and resources, they need accurate and complete data reflecting program activities. We are currently reviewing the accuracy and completeness of Coast Guard compliance data and will report on this issue later this year.

TSA Has Made Progress in Implementing the TWIC Program, but Key Deadline Has Been Missed as TSA Evaluates Test Program

The Secretary of DHS was required by MTSA to, among other things, issue a Transportation Worker Identification Card that uses biometrics, such as fingerprints, to control access to secure areas of seaports and vessels. TSA had already initiated a program to create an identification credential that could be used by workers in all modes of transportation when MTSA was enacted. This program, called the TWIC program, is designed to collect personal and biometric information to validate workers' identities, conduct background checks on transportation workers to ensure they do not pose a threat to security, issue tamper-resistant biometric credentials that cannot be counterfeited, verify these credentials using biometric access control systems before a worker is granted unescorted access to a secure area, and revoke credentials if disqualifying information is discovered, or if a card is lost, damaged, or stolen. TSA, in partnership with the Coast Guard, is focusing initial implementation on the maritime sector.

We have previously reported on the status of this program and the challenges that it faces.[28] Most recently, we reported that TSA has made progress in implementing the TWIC program and addressing problems we previously identified regarding contract planning and oversight and coordination with stakeholders.[29] For example, TSA reported that it added staff with program and contract management expertise to help oversee the contract and developed plans for conducting public outreach and education efforts.

The SAFE Port Act required TSA to implement TWIC at the 10 highest-risk ports by July 1, 2007, conduct a pilot program to test TWIC access control technologies

in the maritime environment; issue regulations requiring TWIC card readers based on the findings of the pilot; and periodically report to Congress on the status of the program. However, TSA did not meet the July 1 deadline, citing the need to conduct additional testing of the systems and technologies that will be used to enroll the estimated 770,000 workers that will be required to obtain a TWIC card. According to TSA officials, the agency plans to complete this testing and begin enrolling workers at the Port of Wilmington in October 2007, and begin enrolling workers at additional ports soon thereafter. TSA is also in the process of conducting a pilot program to test TWIC access control technologies in the maritime environment that will include a variety of maritime facilities and vessels in multiple geographic locations. According to TSA, the results of the pilot program will help the agency issue future regulations that will require the installation of access control systems necessary to read the TWIC cards.

It is important that TSA establish clear and reasonable time-frames for implementing TWIC as the agency begins enrolling workers and issuing TWIC cards in October. TSA could face additional challenges as the TWIC implementation progresses; these include monitoring the effectiveness of contract planning and oversight. TSA has developed a quality assurance surveillance plan with performance metrics that the enrollment contractor must meet to receive payment. The agency has also taken steps to strengthen government oversight of the TWIC contract by adding staff with program and contract management expertise. However, the effectiveness of these steps will not be clear until implementation of the TWIC program begins. Ensuring a successful enrollment process for the program presents another challenge. According to TSA, the agency has made communication and coordination top priorities by taking actions such as establishing a TWIC stakeholder communication committee and requiring the enrollment contractor to establish a plan for coordinating and communicating with all stakeholders who will be involved in the program. Finally, TSA will have to address access control technologies to ensure that the program is implemented effectively. It will be important that TSA's TWIC access control technology pilot ensure that these technologies work effectively in the maritime environment before facilities and vessels will be required to implement them.

DHS Working to Coordinate Multiple Background Check Programs for Transportation Workers

Since the terrorist attacks on September 11, the Federal Government has taken steps to ensure that transportation workers, many of whom transport hazardous materials or have access to secure areas in locations such as ports, are properly screened to ensure they do not pose a security risk. Concerns have been raised, however, that transportation workers may face a variety of background checks, each with different standards. In July 2004, the 9/11 Commission reported that having too many different biometric standards, travel facilitation systems, credentialing systems, and screening requirements hampers the development of information crucial for stopping terrorists from entering the country, is expensive, and is inefficient.[30] The Commission recommended that a coordinating body raise standards, facilitate information-sharing, and survey systems for potential problems. In August 2004, Homeland Security Presidential Directive 11 announced a new U.S. policy to "implement a coordinated and comprehensive approach to terrorist-related screening—in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure—that supports homeland security, at home and abroad."

DHS components have begun a number of their own background check initiatives. For example, in January 2007, TSA determined that the background checks required for three other DHS programs satisfied the background check requirement for the TWIC program.[31] That is, an applicant who has already undergone a background check in association with any of these three programs does not have to undergo an additional background check and pays a reduced fee to obtain a TWIC card. Similarly, the Coast Guard plans to consolidate four credentials and require that all pertinent information previously submitted by an applicant at a Coast Guard Regional Examination Center will be forwarded by the center to TSA through the TWIC enrollment process.

In April 2007, we completed a study of DHS background check programs as part of a SAFE Port Act requirement to do so.[32] We found that the six programs we reviewed were conducted independently of one another, collected similar information, and used similar background check processes. Further, each program operated separate enrollment facilities to collect background information and did not share it with the other programs. We also found that DHS did not track the number of workers who, needing multiple credentials, were subjected to multiple background check pro-

grams. Because DHS is responsible for a large number of background check programs, we recommended that DHS ensure that its coordination plan includes implementation steps, time-frames, and budget requirements; discusses potential costs/benefits of program standardization; and explores options for coordinating and aligning background checks within DHS and other Federal agencies.

DHS concurred with our recommendations and continues to take steps—both at the department level and within its various agencies—to consolidate, coordinate, and harmonize such background check programs.[33] At the department level, DHS created SCO in July 2006 to coordinate DHS background check programs. SCO is in the early stages of developing its plans for this coordination. In December 2006, SCO issued a report identifying common problems, challenges, and needed improvements in the credentialing programs and processes across the department. The office awarded a contract in April 2007 that will provide the methodology and support for developing an implementation plan to include common design and comparability standards and related milestones to coordinate DHS screening and credentialing programs. Since April 2007, DHS and SCO signed a contract to produce three deliverables to align its screening and credentialing activities, set a method and time-frame for applying a common set of design and comparability standards, and eliminate redundancy through harmonization. These three deliverables are as follows:

- Credentialing framework: A framework completed in July 2007 that describes a credentialing life-cycle of registration and enrollment, eligibility vetting and risk assessment, issuance, expiration and revocation, and redress. This framework was to incorporate risk-based levels or criteria, and an assessment of the legal, privacy, policy, operational, and technical challenges.
- Technical review: An assessment scheduled for completion in October 2007 is to be completed by the contractor in conjunction with the DHS Office of the Chief Information Officer. This is to include a review of the issues present in the current technical environment and the proposed future technical environment needed to address those issues, and provide recommendations for targeted investment reuse and key target technologies.
- Transition plan: A plan scheduled to be completed in November 2007 is to outline the projects needed to actualize the framework, including identification of major activities, milestones, and associated timeline and costs.

Stakeholders in this effort include multiple components of DHS and the Departments of State and Justice.

In addition, the DHS Office of the Chief Information Officer (CIO) and the Director of SCO issued a memo in May 2007 to promote standardization across screening and credentialing programs. In this memo, DHS indicated that: (1) programs requiring the collection and use of fingerprints to vet individuals will use the Automated Biometric Identification System (IDENT); (2) these programs are to reuse existing or currently planned and funded infrastructure for the intake of identity information to the greatest extent possible; (3) its CIO is to establish a procurement plan to ensure that the department can handle a large volume of automated vetting from programs currently in the planning phase; and (4) to support the sharing of databases and potential consolidation of duplicative applications, the Enterprise Data Management Office is currently developing an inventory of biographic data assets that DHS maintains to support identity management and screening processes.

While continuing to consolidate, coordinate, and harmonize background check programs, DHS will likely face additional challenges, such as ensuring that its plans are sufficiently complete without being overly restrictive, and lack of information regarding the potential costs and benefits associated with the number of redundant background checks. SCO will be challenged to coordinate DHS's background check programs in such a way that any common set of standards developed to eliminate redundant checks meets the varied needs of all the programs without being so strict that it unduly limits the applicant pool or so intrusive that potential applicants are unwilling to take part. Without knowing the potential costs and benefits associated with the number of redundant background checks that harmonization would eliminate, DHS lacks the performance information that would allow its program managers to compare their program results with goals. Thus, DHS cannot be certain where to target program resources to improve performance. As we recommended, DHS could benefit from a plan that includes, at a minimum, a discussion of the potential costs and benefits associated with the number of redundant background checks that would be eliminated through harmonization.

Container Security Programs Continue to Expand and Mature, but New Challenges Emerge

Through the development of strategic plans, human capital strategies, and performance measures, several container security programs have been established and matured. However, these programs continue to face technical and management challenges in implementation. As part of its layered security strategy, CBP developed the Automated Targeting System as a decision-support tool to assess the risks of individual cargo containers. ATS is a complex mathematical model that uses weighted rules that assign a risk score to each arriving shipment based on shipping information (*e.g.,* manifests, bills of lading, and entry data). Although the program has faced quality assurance challenges from its inception, CBP has made significant progress in addressing these challenges. CBP's in-bond program does not collect detailed information at the U.S. port of arrival that could aid in identifying cargo posing a security risk and promote the effective use of inspection resources. In the past, CSI has lacked sufficient staff to meet program requirements. C–TPAT has faced challenges with validation quality and management in the past, in part due to its rapid growth. The Department of Energy's (DOE) Megaports Initiative faces ongoing operational and technical challenges in the installation and maintenance of radiation detection equipment at ports. In addition, implementing the Secure Freight Initiative and the 9/11 Commission Act of 2007 presents additional challenges for the scanning of cargo containers inbound to the United States.

Management of the Automated Targeting System Has Improved

CBP is responsible for preventing terrorists and weapons of mass destruction from entering the United States. As part of this responsibility, CBP addresses the potential threat posed by the movement of oceangoing cargo containers. To perform this mission, CBP officers at seaports utilize officer knowledge and CBP automated systems to assist in determining which containers entering the country will undergo inspections, and then perform the necessary level of inspection of each container based upon risk. To assist in determining which containers are to be subjected to inspection, CBP uses a layered security strategy that attempts to focus resources on potentially risky cargo shipped in containers while allowing other ocean going containers to proceed without disrupting commerce. ATS is one key element of this strategy. CBP uses ATS as a decision-support tool to review documentation, including electronic manifest information submitted by the ocean carriers on all arriving shipments, and entry data submitted by brokers to develop risk scores that help identify containers for additional inspection.[34] CBP requires the carriers to submit manifest information 24 hours prior to a United States-bound sea container being loaded onto a vessel in a foreign port. CBP officers use these scores to help them make decisions on the extent of documentary review or additional inspection as required.

We have conducted several reviews of ATS and made recommendations for its improvement.[35] Consistent with these recommendations, CBP has implemented a number of important internal controls for the administration and implementation of ATS.[36] For example, CBP (1) has established performance metrics for ATS, (2) is manually comparing the results of randomly conducted inspections with the results of inspections resulting from ATS analysis of the shipment data, and (3) has developed and implemented a testing and simulation environment to conduct computer-generated tests of ATS. Since our last report on ATS, the SAFE Port Act required that the CBP Commissioner take additional actions to further improve ATS. These requirements included steps such as (1) having an independent panel review the effectiveness and capabilities of ATS; (2) considering future iterations of ATS that would incorporate smart features;[37] (3) ensuring that ATS has the capability to electronically compare manifest and other available data to detect any significant anomalies and facilitate their resolution; (4) ensuring that ATS has the capability to electronically identify, compile, and compare select data elements following a maritime transportation security incident; and (5) developing a schedule to address recommendations made by GAO and the Inspectors General of the Department of the Treasury and DHS.

CBP's Management of the In-Bond Cargo System Impedes Efforts to Manage Security Risks

CBP's in-bond system—which allows goods to transit the United States without officially entering U.S. commerce—must balance the competing goals of providing port security, facilitating trade, and collecting trade revenues. However, we have earlier reported that CBP's management of the system has impeded efforts to manage security risks. Specifically, CBP does not collect detailed information on in-bond

cargo at the U.S. port of arrival that could aid in identifying cargo posing a security risk and promote effective use of inspection resources.[38]

The in-bond system is designed to facilitate the flow of trade throughout the United States and is estimated to be widely used. The U.S. customs system allows cargo to move from the U.S. arrival port, without appraisal or payment of duties to another U.S. port for official entry into U.S. commerce or for exportation.[39] In-bond regulations currently permit bonded carriers from 15 to 60 days, depending on the mode of shipment, to reach their final destination and allow them to change a shipment's final destination without notifying CBP. The in-bond system allows the trade community to avoid congestion and delays at U.S. seaports whose infrastructure has not kept pace with the dramatic growth in trade volume. In-bond facilitates trade by allowing importers and shipping agents the flexibility to move cargo more efficiently. Using the number of in-bond transactions reported by CBP for the 6-month period of October 2004 to March 2005, we found over 6.5 million in-bond transactions were initiated nationwide. Some CBP port officials have estimated that in-bond shipments represent from 30 percent to 60 percent of goods received at their ports.[40]

As discussed earlier in this testimony, CBP uses manifest information it receives on all cargo arriving at U.S. ports (including in-bond cargo) as input for ATS scoring to aid in identifying security risks and setting inspection priorities. For regular cargo, the ATS score is updated with more detailed information as the cargo makes official entry at the arrival port. For in-bond cargo, the ATS scores generally are not updated until these goods move from the port of arrival to the destination port for official entry into United States commerce, or not updated at all for cargo that is intended to be exported.[41] As a result, in-bond goods might transit the United States without having the most accurate ATS risk score.

Entry information frequently changes the ATS score for in-bond goods.[42] For example, CBP provided data for four major ports comparing the ATS score assigned to in-bond cargo at the port of arrival based on the manifest to the ATS score given after goods made official entry at the destination port.[43] These data show that for the four ports, the ATS score based on the manifest information stayed the same an average of 30 percent of the time after being updated with entry information, ATS scores increased an average of 23 percent of the time and decreased an average of 47 percent of the time. A higher ATS score can result in higher priority being given to cargo for inspection than otherwise would be given based solely on the manifest information. A lower ATS score can result in cargo being given a lower priority for inspection and potentially shift inspection resources to cargo deemed a higher security risk. Without having the most accurate ATS score, in-bond goods transiting the United States pose a potential security threat because higher-risk cargo may not be identified for inspection at the port of arrival. In addition, scarce inspection resources may be misdirected to in-bond goods that a security score based on better information might have shown did not warrant inspection.

We earlier recommended that the Commissioner of CBP take action in three areas to improve the management of the in-bond program, which included collecting and using improved information on in-bond shipments to update the ATS score for in-bond movements at the arrival port and enable better informed decisions affecting security, trade and revenue collection.[44] DHS agreed with most of our recommendations.[45] According to CBP, they are in the process of developing an in-bond weight set to be utilized to further identify cargo posing a security risk. The weight set is being developed based on expert knowledge, analysis of previous in-bond seizures, and creation of rules based on in-bond concepts.

The SAFE Port Act of 2006 contains provisions related to securing the international cargo supply chain, including provisions related to the movement of in-bond cargo. Specifically, it requires that CBP submit a report to several Congressional committees on the in-bond system that includes an assessment of whether ports of arrival should require additional information for in-bond cargo, a plan for tracking in-bond cargo in CBP's Automated Commercial Environment information system, and assessment of the personnel required to ensure reconciliation of in-bond cargo between arrival port and destination port. The report must also contain an assessment of the feasibility of reducing transit time while traveling in-bond, and an evaluation of the criteria for targeting and examining in-bond cargo. Although the report was due June 30, 2007, CBP has not yet finalized the report and released it to Congress.

The CSI Program Continues to Mature, but Addressing SAFE Port Act Requirements Adds New Challenges

CPB initiated its CSI program to detect and deter terrorists from smuggling weapons of mass destruction (WMD) via cargo containers before they reach domestic

seaports in January 2002. The SAFE Port Act formalized the CSI program into law. Under CSI, foreign governments sign a bilateral agreement with CBP to allow teams of U.S. customs officials to be stationed at foreign seaports to identify cargo container shipments at risk of containing WMD. CBP personnel use automated risk assessment information and intelligence to target and identify those at risk containing WMD. When a shipment is determined to be high risk, CBP officials refer it to host government officials who determine whether to examine the shipment before it leaves their seaport for the United States. In most cases, host government officials honor the U.S. request by examining the referred shipments with nonintrusive inspection equipment and, if they deem necessary, by opening the cargo containers to physically search the contents inside.[46] CBP planned to have a total of 58 seaports by the end of Fiscal Year 2007.

Our 2003 and 2005 reports on the CSI program found both successes and challenges faced by CBP in implementing the program.[47] Since our last CSI report in 2005, CBP has addressed some of the challenges we identified and has taken steps to improve the CSI program. Specifically, CBP contributed to the Strategy to Enhance International Supply Chain Security that DHS issued in July 2007, which addressed a SAFE Port Act requirement and filled an important gap—between broad national strategies and program-specific strategies, such as for CSI—in the strategic framework for maritime security that has evolved since 9/11. In addition, in 2006 CBP issued a revised CSI strategic plan for 2006 to 2011, which added three critical elements that we had identified in our April 2005 report as missing from the plan's previous iteration. In the revised plan, CBP described how performance goals and measures are related to CSI objectives, how CBP evaluates CSI program operations, and what external factors beyond CBP's control could affect program operations and outcomes. Also, by expanding CSI operations to 58 seaports by the end of September 2007, CBP would have met its objective of expanding CSI locations and program activities. CBP projected that at the end of Fiscal Year 2007 between 85 and 87 percent of all U.S.-bound shipments in containers will pass through CSI ports where the risk level of the container cargo is assessed and the contents are examined as deemed necessary.

Although CBP's goal is to review information about all U.S.-bound containers at CSI seaports for high-risk contents before the containers depart for the United States, we reported in 2005 that the agency has not been able to place enough staff at some CSI ports to do so.[48] Also, the SAFE Port Act required DHS to develop a human capital management plan to determine adequate staffing levels in U.S. and CSI ports. CBP has developed a human capital plan, increased the number of staff at CSI ports, and provided additional support to the deployed CSI staff by using staff in the United States to screen containers for various risk factors and potential inspection. With these additional resources, CBP reports that manifest data for all U.S.-bound container cargo are reviewed using ATS to determine whether the container is at high risk of containing WMD. However, the agency faces challenges in ensuring that optimal numbers of staff are assigned to CSI ports due in part to its reliance on placing staff overseas at CSI ports without systematically determining which functions could be performed overseas and which could be performed domestically.

Also, in 2006 CBP improved its methods for conducting onsite evaluations of CSI ports, in part by requiring CSI teams at the seaports to demonstrate their proficiency at conducting program activities and by employing electronic tools designed to assist in the efficient and systematic collection and analysis of data to help in evaluating the CSI team's proficiency. In addition, CBP continued to refine the performance measures it uses to track the effectiveness of the CSI program by streamlining the number of measures it uses to six, modifying how one measure is calculated to address an issue we identified in our April 2005 report; and developing performance targets for the measures. We are continuing to review these assessment practices as part of our ongoing review of the CSI program, and expect to report on the results of this effort shortly.

Similar to our recommendation in a previous CSI report, the SAFE Port Act called upon DHS to establish minimum technical criteria for the use of nonintrusive inspection equipment in conjunction with CSI. The Act also directs DHS to require that seaports receiving CSI designation operate such equipment in accordance with these criteria and with standard operating procedures developed by DHS. CBP officials stated that their agency faces challenges in implementing this requirement due to sovereignty issues and the fact that the agency is not a standard setting organization, either for equipment or for inspections processes or practices. However, CBP has developed minimum technical standards for equipment used at domestic ports and the World Customs Organization (WCO)[49] had described issues—not standards—to consider when procuring inspection equipment. Our work suggests that

CBP may face continued challenges establishing equipment standards and monitoring host government operations, which we are also examining in our ongoing review of the CSI program.

C–TPAT Continues to Expand and Mature, but Management Challenges Remain

CBP initiated C–TPAT in November 2001 to complement other maritime security programs as part of the agency's layered security strategy. In October 2006, the SAFE Port Act formalized C–TPAT into law. C–TPAT is a voluntary program that enables CBP officials to work in partnership with private companies to review the security of their international supply chains and improve the security of their shipments to the United States. In return for committing to improve the security of their shipments by joining the program, C–TPAT members receive benefits that result in the likelihood of reduced scrutiny of their shipments, such as a reduced number of inspections or shorter wait times for their shipments. CBP uses information about C–TPAT membership to adjust risk-based targeting of these members shipments in ATS. As of July 2007, CBP had certified more than 7,000 companies that import goods via cargo containers through U.S. seaports—which accounted for approximately 45 percent of all U.S. imports—and validated the security practices of 78 percent of these certified participants.

We reported on the progress of the C–TPAT program in 2003 and 2005 and recommended that CBP develop a strategic plan and performance measures to track the program's status in meeting its strategic goals.[50] DHS concurred with these recommendations. The SAFE Port Act also mandated that CBP develop and implement a 5-year strategic plan with outcome-based goals and performance measures for C–TPAT. CBP officials stated that they are in the process of updating their strategic plan for C–TPAT, which was issued in November 2004, for 2007 to 2012. This updated plan is being reviewed within CBP, but a time-frame for issuing the plan has not been established. We recommended in our March 2005 report that CBP establish performance measures to track its progress in meeting the goals and objectives established as part of the strategic planning process.[51] Although CBP has since put additional performance measures in place, CBP's efforts have focused on measures regarding program participation and facilitating trade and travel. CBP has not yet developed performance measures for C–TPAT's efforts aimed at ensuring improved supply chain security, which is the program's purpose.

In our previous work, we acknowledged that the C–TPAT program holds promise as part of a layered maritime security strategy. However, we also raised a number of concerns about the overall management of the program. Since our past reports, the C–TPAT program has continued to mature. The SAFE Port Act mandated that actions—similar to ones we had recommended in our March 2005 report—be taken to strengthen the management of the program. For example, the Act included a new goal that CBP make a certification determination within 90 days of CBP's receipt of a C–TPAT application, validate C–TPAT members' security measures and supply chain security practices within 1 year of their certification, and revalidate those members no less than once in every 4 years. As we recommended in our March 2005 report, CBP has developed a human capital plan and implemented a records management system for documenting key program decisions. CBP has addressed C–TPAT staffing challenges by increasing the number of supply chain security specialists from 41 in 2005 to 156 in 2007.

In February 2007, CBP updated its resource needs to reflect SAFE Port Act requirements, including that certification, validation, and revalidation processes be conducted within specified time-frames. CBP believes that C–TPAT's current staff of 156 supply chain security specialists will allow it to meet the Act's initial validation and revalidation goals for 2007 and 2008. If an additional 50 specialists authorized by the Act are made available by late 2008, CBP expects to be able to stay within compliance of the Act's time-frame requirements through 2009. In addition, CBP developed and implemented a centralized electronic records management system to facilitate information storage and sharing and communication with C–TPAT partners. This system—known as the C–TPAT Portal—enables CBP to track and ascertain the status of C–TPAT applicants and partners to ensure that they are certified, validated, and revalidated within required time-frames. As part of our ongoing work, we are reviewing the data captured in Portal, including data needed by CBP management to assess the efficiency of C–TPAT operations and to determine compliance with its program requirements. These actions—dedicating resources to carry out certification and validation reviews and putting a system in place to track the timeliness of these reviews—should help CBP meet several of the mandates of the SAFE Port Act. We expect to issue a final report documenting results of this work shortly.

Our 2005 report raised concerns about CBP granting benefits prematurely—before CBP had validated company practices. Related to this, the SAFE Port Act codified CBP's policy of granting graduated benefits to C–TPAT members. Instead of granting new members full benefits without actual verification of their supply chain security, CBP implemented three tiers to grant companies graduated benefits based on CBP's certification and validation of their security practices. Tier 1 benefits—a limited reduction in the score assigned in ATS—are granted to companies upon certification that their written description of their security profile meets minimum security criteria. Companies whose security practices CBP validates in an on-site assessment receive Tier 2 benefits that may include reduced scores in ATS, reduced cargo examinations, and priority searches of cargo. If CBP's validation shows sustained commitment by a company to security practices beyond what is expected, the company receives Tier 3 benefits. Tier 3 benefits may include expedited cargo release at U.S. ports at all threat levels, further reduction in cargo examinations, priority examinations, and participation in joint incident management exercises.

Our 2005 report also raised concerns about whether the validation process was rigorous enough. Similarly, the SAFE Port Act mandates that the validation process be strengthened, including setting a year time-frame for completing validations. CBP initially set a goal of validating all companies within their first 3 years as C–TPAT members, but the program's rapid growth in membership made the goal unachievable. CBP then moved to a risk-based approach to selecting members for validation, considering factors such as a company's having foreign supply chain operations in a known terrorist area or involving multiple foreign suppliers. CBP further modified its approach to selecting companies for validation to achieve greater efficiency by conducting "blitz" operations to validate foreign elements of multiple members' supply chains in a single trip. Blitz operations focus on factors such as C–TPAT members within a certain industry, supply chains within a certain geographic area, or foreign suppliers to multiple C–TPAT members. Risks remain a consideration, according to CBP, but the blitz strategy drives the decision of when a member company will be validated. In addition to taking these actions to efficiently conduct validations, CBP has periodically updated the minimum security requirements that companies must meet to be validated and is conducting a pilot program of using third-party contractors to conduct validation assessments. As part of our ongoing work, we are reviewing these actions, which are required as part of the SAFE Port Act, and other CBP efforts to enhance its C–TPAT validation process.

CBP Has Played a Key Role in Promoting Global Customs Security Standards and Initiatives, but Progress with These Efforts Presents New Challenges for CSI and C–TPAT

The CSI and C–TPAT programs have provided a model for global customs security standards, but as other countries adopt the core principles of CSI and programs similar to C–TPAT, CBP may face new challenges. Foreign officials within the World Customs Organization and elsewhere have observed the CSI and C–TPAT programs as potential models for enhancing supply chain security. Also, CBP has taken a lead role in working with members of the domestic and international customs and trade community on approaches to standardizing supply chain security worldwide. As CBP has recognized, and we have previously reported, in security matters the United States is not self-contained, in either its problems or its solutions. The growing interdependence of nations requires policymakers to recognize the need to work in partnerships across international boundaries to achieve vital national goals.

For this reason, CBP has committed through its strategic planning process to develop and promote an international framework of standards governing customs-to-customs relationships and customs-to-business relationships in a manner similar to CSI and C–TPAT, respectively. To achieve this, CBP has worked with foreign customs administrations through the WCO to establish a framework creating international standards that provide increased security of the global supply chain while facilitating international trade. The member countries of the WCO, including the United States, adopted such a framework, known as the WCO Framework of Standards to Secure and Facilitate Global Trade and commonly referred to as the SAFE Framework, in June 2005. The SAFE Framework internationalizes the core principles of CSI in creating global standards for customs security practices and promotes international customs-to-business partnership programs, such as C–TPAT. As of September 11, 2007, 148 WCO member countries had signed Letters of Intent to implement the SAFE Framework. CBP, along with the customs administrations of other countries and through the WCO, provides technical assistance and training to those countries that want to implement the SAFE Framework, but do not yet have the capacity to do so.

The SAFE Framework enhances the CSI program by promoting the implementation of CSI-like customs security practices, including the use of electronic advance information requirements and risk-based targeting, in both CSI and non-CSI ports worldwide. The framework also lays the foundation for mutual recognition, an arrangement whereby one country can attain a certain level of assurance about the customs security standards and practices and business partnership programs of another country. In June 2007, CBP entered into the first mutual recognition arrangement of a business-to-customs partnership program with the New Zealand Customs Service. This arrangement stipulates that members of one country's business-to-customs program be recognized and receive similar benefits from the customs service of the other country. CBP is pursuing similar arrangements with Jordan and Japan, and is conducting a pilot program with the European Commission to test approaches to achieving mutual recognition and address differences in their respective programs. However, the specific details of how the participating counties' customs officials will implement the mutual recognition arrangement—such as what benefits, if any, should be allotted to members of other countries' C-TPAT like programs—have yet to be determined. As CBP goes forward, it may face challenges in defining the future of its CSI and C–TPAT programs and, more specifically, in managing the implementation of mutual recognition arrangements, including articulating and agreeing to the criteria for accepting another country's program; the specific arrangements for implementation, including the sharing of information; and the actions for verification, enforcement; and, if necessary, termination of the arrangement.

DOE Continues to Expand Its Megaports Program

The Megaports Initiative, initiated by DOE's National Nuclear Security Administration in 2003, represents another component in the efforts to prevent terrorists from smuggling WMD in cargo containers from overseas locations. The goal of this initiative is to enable foreign government personnel at key foreign seaports to use radiation detection equipment to screen shipping containers entering and leaving these ports, regardless of the containers' destination, for nuclear and other radioactive material that could be used against the United States or its allies. DOE installs radiation detection equipment, such as radiation portal monitors and handheld radioactive isotope identification devices, at foreign seaports that is then operated by foreign government officials and port personnel working at these ports.

Through August 2007, DOE had completed installation of radiation detection equipment at eight ports: Rotterdam, the Netherlands; Piraeus, Greece; Colombo, Sri Lanka; Algeciras, Spain; Singapore; Freeport, Bahamas; Manila, Philippines; and Antwerp, Belgium (Phase I). Operational testing is under way at four additional ports: Antwerp, Belgium (Phase II); Puerto Cortes, Honduras; Qasim, Pakistan; and Laem Chabang, Thailand. Additionally, DOE has signed agreements to begin work and is in various stages of implementation at ports in 12 other countries, including the United Kingdom, United Arab Emirates/Dubai, Oman, Israel, South Korea, China, Egypt, Jamaica, the Dominican Republic, Colombia, Panama, and Mexico, as well as Taiwan and Hong Kong. Several of these ports are also part of the Secure Freight Initiative, discussed in the next section. Further, in an effort to expand cooperation, DOE is engaged in negotiations with approximately 20 additional countries in Europe, Asia, the Middle East, and Latin America.

DOE had made limited progress in gaining agreements to install radiation detection equipment at the highest priority seaports when we reported on this program in March 2005.[52] Then, the agency had completed work at only two ports and signed agreements to initiate work at five others. We also noted that DOE's cost projections for the program were uncertain, in part because they were based on DOE's $15 million estimate for the average cost per port. This per port cost estimate may not be accurate because it was based primarily on DOE's radiation detection assistance work at Russian land borders, airports, and seaports and did not account for the fact that the costs of installing equipment at individual ports vary and are influenced by factors such as a port's size, physical layout, and existing infrastructure. Since our review, DOE has developed a strategic plan for the Megaports Initiative and revised it's per port estimates to reflect port size, with per port estimates ranging from $2.6 million to $30.4 million.

As we earlier reported, DOE faces several operational and technical challenges specific to installing and maintaining radiation detection equipment at foreign ports as the agency continues to implement its Megaports Initiative. These challenges include ensuring the ability to detect radioactive material, overcoming the physical layout of ports and cargo-stacking configurations, and sustaining equipment in port environments with high winds and sea spray.

Secure Freight Initiative Testing Feasibility of Combining Scanning Technologies

The SAFE Port Act required that a pilot program—known as the Secure Freight Initiative (SFI)—be conducted to determine the feasibility of 100 percent scanning of U.S.-bound containers. To fulfill this requirement, CBP and DOE jointly announced the formation of SFI in December 2006, as an effort to build upon existing port security measures by enhancing the U.S. Government's ability to scan containers for nuclear and radiological materials overseas and better assess the risk of inbound containers. In essence, SFI builds upon the CSI and Megaports programs. The SAFE Port Act specified that new integrated scanning systems that couple nonintrusive imaging equipment and radiation detection equipment must be pilot-tested. It also required that, once fully implemented, the pilot integrated scanning system scan 100 percent of containers destined for the United States that are loaded at pilot program ports.

According to agency officials, the initial phase of the initiative will involve the deployment of a combination of existing container scanning technology—such as X-ray and gamma ray scanners used by host nations at CSI ports to locate high-density objects that could be used to shield nuclear materials, inside containers—and radiation detection equipment. The ports chosen to receive this integrated technology are: Port Qasim in Pakistan, Puerto Cortes in Honduras, and Southampton in the United Kingdom. Four other ports located in Hong Kong, Singapore, the Republic of Korea, and Oman will receive more limited deployment of these technologies as part of the pilot program. According to CBP, containers from these ports will be scanned for radiation and other risk factors before they are allowed to depart for the United States. If the scanning systems indicate that there is a concern, both CSI personnel and host country officials will simultaneously receive an alert and the specific container will be inspected before that container continues to the United States. CBP officials will determine which containers are inspected, either on the scene locally or at CBP's National Targeting Center.

Per the SAFE Port Act, CBP is to report by April 2008 on, among other things, the lessons learned from the SFI pilot ports and the need for and the feasibility of expanding the system to other CSI ports. Every 6 months thereafter, CBP is to report on the status of full-scale deployment of the integrated scanning systems to scan all containers bound for the United States before their arrival.

New Requirement for 100 Percent Scanning Introduces New Challenges

Recent legislative actions have updated U.S. maritime security requirements and may affect overall international maritime security strategy. In particular, the recently enacted Implementing Recommendations of the 9/11 Commission Act (9/11 Act) requires, by 2012, 100 percent scanning of U.S.-bound cargo containers using nonintrusive imaging equipment and radiation detection equipment at foreign seaports. The Act also specifies conditions for potential extensions beyond 2012 if a seaport cannot meet that deadline. Additionally, it requires the Secretary of DHS to develop technological and operational standards for scanning systems used to conduct 100 percent scanning at foreign seaports. The Secretary also is required to ensure that actions taken under the Act do not violate international trade obligations and are consistent with the WCO SAFE Framework. The 9/11 Act provision replaces the requirement of the SAFE Port Act that called for 100 percent scanning of cargo containers before their arrival in the United States, but required implementation as soon as possible rather than specifying a deadline. While we have not yet reviewed the implementation of the 100 percent scanning requirement, we have a number of preliminary observations based on field visits of foreign ports regarding potential challenges CBP may face in implementing this requirement:

- *CBP may face challenges balancing new requirement with current international risk management approach.* CBP may have difficulty requiring 100 percent scanning while also maintaining a risk-based security approach that has been developed with many of its international partners. Currently, under the CSI program, CBP uses automated targeting tools to identify containers that pose a risk for terrorism for further inspection before being placed on vessels bound for the United States. As we have previously reported, using risk management allows for reduction of risk against possible terrorist attack to the Nation given resources allocated and is an approach that has been accepted governmentwide. Furthermore, many U.S. and international customs officials we have spoken to, including officials from the World Customs Organization, have stated that the 100 percent scanning requirement is contrary to the SAFE Framework developed and implemented by the international customs community, including CBP. The SAFE Framework, based on CSI and C–TPAT, calls for a risk man-

agement approach, whereas the 9/11 Act calls for the scanning of all containers regardless of risk.

- *United States may not be able to reciprocate if other countries request it.* The CSI program, whereby CBP officers are placed at foreign seaports to target cargo bound for the United States, is based on a series of bilateral, reciprocal agreements with foreign governments. These reciprocal agreements also allow foreign governments the opportunity to place customs officials at U.S. seaports and request inspection of cargo containers departing from the United States and bound for their home country. Currently, customs officials from certain countries are stationed at domestic seaports and agency officials have told us that CBP has inspected 100 percent of containers that these officials have requested for inspection. According to CBP officials, the SFI pilot, as an extension of the CSI program, allows foreign officials to ask the United States to reciprocate and scan 100 percent of cargo containers bound for those countries. Although the Act establishing the 100 percent scanning requirement does not mention reciprocity, CBP officials have told us that the agency does not have the capacity to reciprocate should it be requested to do so, as other government officials have indicated they might when this provision of the 9/11 Act is in place.
- *Logistical feasibility is unknown and may vary by port.* Many ports may lack the space necessary to install additional equipment needed to comply with the requirement to scan 100 percent of U.S.-bound containers. Additionally, we observed that scanning equipment at some seaports is located several miles away from where cargo containers are stored, which may make it time consuming and costly to transport these containers for scanning. Similarly, some seaports are configured in such a way that there are no natural bottlenecks that would allow for equipment to be placed such that all outgoing containers can be scanned and the potential to allow containers to slip by without scanning may be possible. Transshipment cargo containers—containers moved from one vessel to another—are only available for scanning for a short period of time and may be difficult to access. Similarly, it may be difficult to scan cargo containers that remain on board a vessel as it passes through a foreign seaport. CBP officials told us that currently containers such as these that are designated as high-risk at CSI ports are not scanned unless specific threat information is available regarding the cargo in that particular container.
- *Technological maturity is unknown.* Integrated scanning technologies to test the feasibility of scanning 100 percent of U.S.-bound cargo containers are not yet operational at all seaports participating in the pilot program, known as SFI. The SAFE Port Act requires CBP to produce a report regarding the program, which will include an evaluation of the effectiveness of scanning equipment at the SFI ports. However, this report will not be due until April 2008. Moreover, agency officials have stated that the amount of bandwidth necessary to transmit scanning equipment outputs to CBP officers for review exceeds what is currently feasible and that the electronic infrastructure necessary to transmit these outputs may be limited at some foreign seaports. Additionally, there are currently no international standards for the technical capabilities of inspection equipment. Agency officials have stated that CBP is not a standard setting organization and has limited authority to implement standards for sovereign foreign governments.
- *Resource responsibilities have not been determined.* The 9/11 Act does not specify who would pay for additional scanning equipment, personnel, computer systems, or infrastructure necessary to establish 100 percent scanning of U.S.-bound cargo containers at foreign ports. According to the Congressional Budget Office (CBO) in its analysis of estimates for implementing this requirement, this provision would neither require nor prohibit the U.S. Federal Government from bearing the cost of conducting scans. For the purposes of its analysis, CBO assumed that the cost of acquiring, installing, and maintaining systems necessary to comply with the 100 percent scanning requirement would be borne by foreign ports to maintain trade with the United States. However, foreign government officials we have spoken to expressed concerns regarding the cost of equipment. They also stated that the process for procuring scanning equipment may take years and can be difficult when trying to comply with changing U.S. requirements. These officials also expressed concern regarding the cost of additional personnel necessary to: (1) operate new scanning equipment; (2) view scanned images and transmit them to the United States; and (3) resolve false alarms. An official from one country with whom we met told us that, while his country does not scan 100 percent of exports, modernizing its customs service to focus more on exports required a 50 percent increase in personnel, and other coun-

tries trying to implement the 100 percent scanning requirement would likely have to increase the size of their customs administrations by at least as much.

- *Use and ownership of data have not been determined.* The 9/11 Act does not specify who will be responsible for managing the data collected through 100 percent scanning of U.S.-bound containers at foreign seaports. However, the SAFE Port Act specifies that scanning equipment outputs from SFI will be available for review by U.S. Government officials either at the foreign seaport or in the United States. It is not clear who would be responsible for collecting, maintaining, disseminating, viewing or analyzing scanning equipment outputs under the new requirement. Other questions to be resolved include ownership of data, how proprietary information would be treated, and how privacy concerns would be addressed.

CBP officials have indicated they are aware that challenges exist. They also stated that the SFI will allow the agency to determine whether these challenges can be overcome. According to senior officials from CBP and international organizations we contacted, 100 percent scanning of containers may divert resources, causing containers that are truly high risk to not receive adequate scrutiny due to the sheer volume of scanning outputs that must be analyzed. These officials also expressed concerns that 100 percent scanning of U.S.-bound containers could hinder trade, leading to long lines and burdens on staff responsible for viewing images. However, given that the SFI pilot program has only recently begun, it is too soon to determine how the 100 percent scanning requirement will be implemented and its overall impact on security.

Agency Comments

We provided a draft of this testimony to DHS agencies and incorporated technical comments as appropriate.

Mr. Chairman and Members of the Committee, this completes my prepared statement. I will be happy to respond to any questions that you or other Members of the Committee have at this time.

Endnotes

[1] Pub. L. 109–347, 120 Stat. 1884 (2006).

[2] Pub. L. 107–295, 116 Stat. 2064 (2002).

[3] The Implementing Recommendations of the 9/11 Commission Act of 2007 amended a SAFE Port Act provision on scanning all United States bound containers at foreign ports. See Pub. L. 110–53, § 1701(a), 121 Stat. 266, 489–90. This amendment is discussed later in this testimony.

[4] A list of related GAO products may be found at the end of this testimony.

[5] The SAFE Port Act did not define "high-priority ports," but the Coast Guard identified a number of factors that it used in determining which ports are high-priority, including risk assessment data, port criticality ratings, and existing investments in facilities.

[6] The Coast Guard has implemented a new field command structure that is designed to unify previously disparate Coast Guard units, such as air stations and marine safety offices, into 35 different integrated commands, called sector command centers. At each of these sectors, the Coast Guard has placed management and operational control of these units and their associated resources under the same commanding officer.

[7] The Coast Guard shares some responsibilities with the U.S. Navy at four of these locations. These centers are located in Hampton Roads, Virginia; Jacksonville, Florida; San Diego, California; and Seattle, Washington.

[8] See GAO, *Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention*, GAO–05–394 (Washington, D.C.: Apr. 15, 2005); *Maritime Security: Enhancements Made, but Implementation and Sustainability Remain Key Challenges,* GAO–05–448T (Washington, D.C.: May 17, 2005); *Maritime Security: Information-Sharing Efforts Are Improving,* GAO–06–933T (Washington, D.C.: July 10, 2006).

[9] According to the Coast Guard, these multiple interagency partners include Customs and Border Protection, Immigration and Customs Enforcement, Department of Defense, the Secure Border Initiative Network (SBInet) Program Office, and State and local partners. A center located in Charleston, South Carolina is managed by the Department of Justice. It was created through an appropriation in the Fiscal Year 2003 Consolidated Appropriations Resolution (Pub. L. 108–7, 117 Stat. 11,53 (2003.)).

[10] *Maritime Security: Observations on Selected Aspects of the SAFE Port Act.* GAO–07–754T. April 26, 2007.

[11] See GAO, *Maritime Security: Information-Sharing Efforts Are Improving,* GAO–06–933T (Washington, D.C.: July 10, 2006); *Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention,* GAO–05–394 (Washington, D.C.: Apr. 15, 2005).

[12] In July 2007, the Coast Guard reported having granted security clearances to 212 area committee members with a need to know, which is an improvement from July 2006, when we reported 188 out of 467 members had received a security clearance to date.

[13] The Coast Guard uses a three-tiered system of Maritime Security (MARSEC) levels consistent with DHS's Homeland Security Advisory System (HSAS). MARSEC levels are designed

to provide a means to easily communicate pre-planned scalable responses to increased threat levels.

[14] NVICs provide detailed guidance about enforcement or compliance with certain Coast Guard safety regulations and programs. NVIC 9–02, most recently revised on October 27, 2005, detailed requirements for area plans.

[15] The MIRP, one of the eight supporting plans of the National Strategy for Maritime Security, is intended to facilitate the restoration of maritime commerce after a terrorist attack or natural disaster.

[16] DHS released the Strategy to Enhance the International Supply Chain in July 2007. This strategy contains a plan to speed the resumption of trade in the event of a terrorist attack on our ports or waterways as required in the SAFE Port Act.

[17] All hazards emergency preparedness efforts seek to prepare all sectors of American society—business, industry and nonprofit; territorial, local, and tribal governments, and the general public—for all hazards the Nation may face, *i.e.,* any large-scale emergency event, including terrorist attacks and natural or accidental disasters.

[18] GAO, *Port Risk Management: Additional Federal Guidance Would Aid Ports in Disaster Planning and Recovery,* GAO–07–412 (Washington, D.C.: Mar. 28, 2007).

[19] GAO, *Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention,* GAO–05–170 (Washington, D.C.: Jan. 14, 2005); and GAO–07–412.

[20] The International Port Security Program uses the ISPS Code as the benchmark by which it measures the effectiveness of a country's anti-terrorism measures in a port. The code was developed after the September 11 attacks and established measures to enhance the security of ships and port facilities with a standardized and consistent security framework. The ISPS code requires facilities to conduct an assessment to identify threats and vulnerabilities and then develop security plans based on the assessment. The requirements of this code are performance-based; therefore compliance can be achieved through a variety of security measures.

[21] In addition to the Coast Guard visiting the ports of foreign countries under this program, countries can also make reciprocal visits to U.S. ports to observe U.S. implementation of the ISPS Code, obtaining ideas for implementation of the code in their ports and sharing best practices for security.

[22] See H.R. Conf. Rep. No. 109–699, at 142 (2006).

[23] There are approximately 140 countries that are maritime trading partners with the United States.

[24] GAO, *Information on Port Security in the Caribbean Basin,* GAO–07–804R, (Washington, D.C.: June 29, 2007).

[25] Requirements for security plans for facilities are found in 33 CFR Part 105, Subpart D.

[26] See GAO, *Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security,* GAO–04–838 (Washington, D.C.: June 2004).

[27] See *GAO, Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making,* GAO–05–97 (Washington, D.C.: September 2005).

[28] See GAO, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program,* GAO–05–106 (Washington, D.C.: December 2004); and *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program,* GAO–06–982 (Washington, D.C.: September 2006).

[29] GAO, *Transportation Security: TSA Has Made Progress in Implementing the Transportation Worker Identification Credential Program, but Challenges Remain,* GAO–07–681T (Washington, D.C.: Apr. 12, 2007).

[30] The National Commission on Terrorist Attacks Upon the United States, *Final Report of the National Commission On Terrorist Attacks Upon the United States,* Washington, D.C.: Jul. 22, 2004).

[31] TSA determined that the background checks required for the hazardous materials endorsement (an endorsement that authorizes an individual to transport hazardous materials for commerce) and the Free and Secure Trade card (a voluntary CBP program that allows commercial drivers to receive expedited border processing) satisfy the background check requirements for TWIC. TSA also determined that an individual issued a Merchant Mariner Document (issued between February 3, 2003, and March 26, 2007) was not subject to an additional background check for TWIC.

[32] The SAFE Port Act required that GAO conduct a study of the background records checks carried out for DHS that are similar to the one required of truck drivers to obtain a hazardous material endorsement. Pub. L. 109–347, § 105 120 Stat. 1884, 1891 (2006). See GAO, *Transportation Security: Efforts to Eliminate Redundant Background Check Investigations,* GAO–07–756 (Washington, D.C.: Apr. 26, 2007).

[33] The term "harmonize" is used to describe efforts to increase efficiency and reduce redundancies by aligning the background check requirements to make the programs more consistent.

[34] Cargo manifests are prepared by the ocean carrier to describe the contents of a container.

[35] The Comptroller General's internal control standards state that internal control activities help ensure that management's directives are carried out. Further, they state that the control objectives should be effective and efficient in accomplishing the agency's control objectives. GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD–00–21.3.1, 11 (Washington, D.C.: November 1999).

[36] The Comptroller General's internal control standards state that internal control activities help ensure that management's directives are carried out. Further, they state that the control objectives should be effective and efficient in accomplishing the agency's control objectives. GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD–00–21.3.1, 11 (Washington, D.C.: November 1999).

[37] Smart features include more complex algorithms and real-time intelligence.

[38] GAO, *International Trade: Persistent Weaknesses in the In-Bond Cargo System Impede Customs and Border Protection's Ability to Address Revenue, Trade, and Security Concerns,* GAO–07–561, (Washington, D.C.: April 17, 2007).

[39] In-bond goods must be transported by a carrier covered by a CBP-approved bond that allows goods that have not yet entered U.S. commerce to move through the United States. The bond is a contract given to ensure performance of obligations imposed by law or regulation and guarantees payment to CBP if these obligations are not performed.

[40] CBP cannot assess the extent of the program because it does not collect accurate information on the value and volume of in-bond cargo, and its analysis of existing data is limited to the number of in-bond transactions.

[41] Although an in-bond form is required for in-bond movement, it does not have the same level of detail contained in entry documents, and data from the form are not used to update ATS scores.

[42] Entry information is documentation to declare items arriving in the United States. Entry information allows CBP to determine what is included in a shipment, and provides more detail on a container's contents than manifest information.

[43] Los Angeles, Long Beach, Newark, and New York.

[44] GAO–07–561.

[45] We made eleven recommendations to improve the management of the in-bond system in three general areas: (1) improving the level of information available on in-bond carge, (2) improving monitoring of in-bond cargo, and (3) improving the efficiency of in-bond compliance measurement programs. DHS agreed with seven of our recommendations, disagreed with three, and stated that one had already been implemented.

[46] A core element of CSI is the use of technology to scan—to capture data including images of cargo container contents—high-risk containers to ensure that examinations can be done rapidly without slowing down the movement of trade. This technology can include equipment such as large scale X-ray and gamma ray machines and radiation detection devices.

[47] See GAO, *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts,* GAO–05–557 (Washington, D.C.: Apr. 26, 2005) and *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors,* GAO–03–770 (Washington, D.C.: July 2003).

[48] GAO–05–557.

[49] The World Customs Organization is an international organization aimed at enhancing the effectiveness and efficiency of customs administrations.

[50] See GAO, *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security,* GAO–05–404 (Washington, D.C.: March 2005); and *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors,* GAO–03–770 (Washington, D.C.: July 2003).

[51] GAO–05–405.

[52] For additional information, see GAO, *Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports,* GAO–05–375 (Washington, D.C.: Mar. 31, 2005).

GAO Related Products

Combating Nuclear Smuggling: Additional Actions Needed to Ensure Adequate Testing of Next Generation of Radiation Detection Equipment. GAO–07–1247T. Washington, D.C.: September 18, 2007.

Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions. GAO–07–1240T. Washington, D.C.: September 18, 2007.

Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions. GAO–07–1081T. Washington, D.C.: September 6, 2007.

Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions. GAO–07–454. Washington, D.C.: August 17, 2007.

Homeland Security: Observations on DHS and FEMA Efforts to Prepare for and Respond to Major and Catastrophic Disasters and Address Related Recommendations and Legislation. GAO–07–1142T. Washington, D.C.: July 31, 2007.

Information on Port Security in the Caribbean Basin. GAO–07–804R. Washington, D.C.: June 29, 2007.

Department of Homeland Security: Science and Technology Directorate's Expenditure Plan. GAO–07–868. Washington, D.C.: June 22, 2007.

Homeland Security: Guidance from Operations Directorate Will Enhance Collaboration among Departmental Operations Centers. GAO–07–683T. Washington, D.C.: June 20, 2007.

Department of Homeland Security: Progress and Challenges in Implementing the Department's Acquisition Oversight Plan. GAO–07–900. Washington, D.C.: June 13, 2007.

Department of Homeland Security: Ongoing Challenges in Creating an Effective Acquisition Organization. GAO–07–948T. Washington, D.C.: June 7, 2007.

Homeland Security: Observations on DHS and FEMA Efforts to Prepare for and Respond to Major and Catastrophic Disasters and Address Related Recommendations and Legislation. GAO–07–835T. Washington, D.C.: May 15, 2007.

Homeland Security: Management and Programmatic Challenges Facing the Department of Homeland Security. GAO–07–833T. Washington, D.C.: May 10, 2007.

Maritime Security: Observations on Selected Aspects of the SAFE Port Act. GAO–07–754T. April 26, 2007.

Transportation Security: DHS Efforts to Eliminate Redundant Background Check Investigations. GAO–07–756. Washington, D.C.: April 26, 2007.

International Trade: Persistent Weaknesses in the In-Bond Cargo System Impede Customs and Border Protection's Ability to Address Revenue, Trade, and Security Concerns. GAO–07–561. Washington, D.C.: April 17, 2007.

Transportation Security: TSA Has Made Progress in Implementing the Transportation Worker Identification Credential Program, but Challenges Remain. GAO–07–681T. Washington, D.C.: April 12, 2007.

Customs Revenue: Customs and Border Protection Needs to Improve Workforce Planning and Accountability. GAO–07–529. Washington, D.C.: April 12, 2007.

Port Risk Management: Additional Federal Guidance Would Aid Ports in Disaster Planning and Recovery. GAO–07–412. Washington, D.C.: March 28, 2007.

Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program. GAO–06–982. Washington, D.C.: September 29, 2006.

Maritime Security: Information-Sharing Efforts Are Improving. GAO–06–933T. Washington, D.C.: July 10, 2006.

Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System. GAO–06–591T. Washington, D.C.: March 30, 2006.

Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making. GAO–05–927. Washington, D.C.: September 9, 2005.

Combating Nuclear Smuggling: Efforts to Deploy Radiation Detection Equipment in the United States and in Other Countries. GAO–05–840T. Washington, D.C.: June 21, 2005.

Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts. GAO–05–557. Washington, D.C.: April 26, 2005.

Homeland Security: Key Cargo Security Programs Can Be Improved. GAO–05–466T. Washington, D.C.: May 26, 2005.

Maritime Security: Enhancements Made, But Implementation and Sustainability Remain Key Challenges. GAO–05–448T. Washington, D.C.: May 17, 2005.

Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security. GAO–05–404. Washington, D.C.: March 11, 2005.

Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention. GAO–05–394. Washington, D.C.: April 15, 2005.

Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports. GAO–05–375. Washington, D.C.: March 30, 2005.

Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges. GAO–05–327. Washington, D.C.: March 2005.

Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention. GAO–05–170. Washington, D.C.: January 14, 2005.

Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program. GAO–05–106. Washington, D.C.: December 2004.

Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security. GAO–04–838. Washington, D.C.: June 2004.

Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection. GAO–04–557T. Washington, D.C.: March 31, 2004.

Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors. GAO–03–770. Washington, D.C.: July 25, 2003.

Senator LAUTENBERG. Thank you, Mr. Caldwell. Mr. Coscia?

STATEMENT OF ANTHONY COSCIA, CHAIRMAN, BOARD OF COMMISSIONERS, THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY

Mr. COSCIA. Mr. Chairman, thank you. Good morning, Vice Chairman Stevens, Senator Lott. Thank you for the opportunity to

testify before this Committee on maritime security and the SAFE Port Act in particular, for many reasons, not the least of which is that we have, for quite a period of time, looked for the leadership to add the level of attention to this issue that we believe it deserves and your efforts here today are very much appreciated by those of us in the field each day.

I'd like to today, talk about briefly several topics related to this issue: cargo security, credentialing, response and recovery and funding and resources. These, as well as other points, were covered in a task force report that was compiled by the Port Authority, assembling a number of key business leaders and government officials in the New Jersey/New York metropolitan area who would be directly impacted by any incident that were to occur and recognizing just how critical this issue is.

First, let me talk a bit about cargo security. When we talk about cargo security, of course, we're talking about securing cargo entering U.S. ports and it is critical to recognize that first and foremost that the ports themselves are not the lone point of vulnerability. The potential for terrorist activity stretches from the cargo's overseas point of origin to where the cargo is placed into a container, to points along the cargo's route to its ultimate destination. Our goal should be to increase our level of confidence that we know the contents of containers before they're even loaded onto a ship destined for a U.S. port. The security process must also include an ability to verify along the route that the container and the cargo have not been tampered with, that the container is transported under the control of responsible parties and that the integrity of the data associated with the movement of the cargo has not been compromised.

We support Section 204 of the SAFE Port Act, which requires minimum standards and procedures for securing containers in transit to the United States. In implementing this section, however, our understanding is that the Department of Homeland Security plans to impose these standards only on importers who enroll in the C–TPAT program. Voluntary cargo security measures are certainly helpful, but Senators, I would submit that they're not clearly sufficient. We must go one step further and make those container security standards, both minimum and mandatory. Importers that choose to go above and beyond the minimum standards should reap the benefits of security and commercial benefits commensurate with their investment in and the effectiveness of their security measures. Those who don't meet minimum standards should be faced with some form of a red lane.

Next, I want to talk briefly about credentialing. I know this is very much the focus of this Committee and I'd like to focus only on several relatively minor but frankly, very critical aspects to the Port Authority and to operators in the field. The current process requires a local match of 25 percent for the implementation of this program, although we clearly recognize that funding and resources are critical at so many levels, we've asked Secretary Chertoff to reconsider this. We have an enormous expense associated with port security at our level. Our agency, since 9/11 has spent over $100 million on port security and this pilot program will require additional expenditures on our side. We're hopeful that this Committee

will support our request to eliminate a 25 percent local matching requirement because there are so many other investments we'll have to make in this program in order for it to be successful, investments which will not be recoverable if the program has to be retooled or is not successful.

Third, I'd like to go on to the issue of response and recovery. We need to develop response and recovery plans but we need to do that in a way that fully incorporates all those who are affected by it. The SAFE Port Act creates an appropriate prioritization scheme for how to develop these plans. We believe more should be done to integrate the way private industry, as well as government levels at varying degrees, work together on developing a comprehensive plan. Any response and recovery plan is relatively ineffective to the extent that 90 or 95 percent of those who are affected by it are not fully integrated into its implementation. Therefore, public and private sectors must collaborate on the development of port-specific plans and procedures in each U.S. port to ensure a timely recovery and effective communication in the aftermath of an incident. These response and recovery plans must be supported by individual business continuity plans and robust training and exercise programs.

Finally and I'm sure it's of no surprise, I would like to make two points regarding security funding. The first is that although there is an effort now to implement 5-year rolling plans with respect to Tier I and Tier II ports, we think that should be extended to all ports to include Tier III and Tier IV ports, therefore we can fully understand on a risk basis, where additional grants should go.

And then finally, our agency feels strongly that there should be some uniform port security fee that should be adopted on a national level. We're not necessarily advocating any particular fee but at present, we're faced with a circumstance where each port is individually making decisions on port security fees. We believe that puts all of us in a position of having to do a balancing act between our competitiveness and providing the adequate level of security. We think on a national level, a uniform fee should be adopted that allows us to comprehensively collect resources and then re-deploy those in the most intelligent way possible to provide the adequate level of security.

Again, thank you for your dedicated attention to this issue. This issue, with leadership, we believe can be addressed very effectively and we applaud yours in that area, Senator.

[The prepared statement of Mr. Coscia follows:]

PREPARED STATEMENT OF ANTHONY COSCIA, CHAIRMAN, BOARD OF COMMISSIONERS, THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY

Chairman Inouye, Vice Chairman Stevens, Senator Lautenberg, Members of the Committee, thank you for the opportunity to testify on the importance of maritime and port security and the implementation of the SAFE Port Act. My name is Anthony Coscia. I am the Chairman of The Port Authority of New York and New Jersey.

The tragic events of September 11 have focused our collective attention on the need to protect our borders at major international gateways like the Port of New York and New Jersey and small ports alike. The Maritime Transportation Security Act of 2002 and the SAFE Port Act are two pieces of landmark legislation that have had a positive impact on our homeland security. However, as we all know, more remains to be done. We commend the entire Senate, and this Committee in particular,

for its work on the SAFE Port Act in devising a layered approach to enhance maritime security.

At the Port Authority we feel that maritime and port security is such an essential matter that we assembled a Task Force of independent non-partisan business and government leaders interested in identifying critical port and supply chain security concerns and promoting ways to resolve or mitigate these concerns. The Task Force issued a report in November 2006 containing our recommendations.

I would like to briefly discuss seven key points relevant to the SAFE Port Act and our Port Security Task Force: (1) the vital nature of our ports; (2) cargo security; (3) credentialing; (4) command and control; (5) response and recovery; (6) research and development; and finally, (7) funding and resources.

The Vital Nature of Ports

Ninety-five percent of the international goods that come into the country come in through our Nation's 361 ports; approximately 13 percent of that volume is handled in the Port of New York and New Jersey alone, the third largest port in the country. The Port generates over 230,000 jobs and $12.6 billion in wages throughout the region. Additionally, the Port contributes $2.1 billion in state and local tax revenues and more than $3.8 billion in Federal tax revenues. Cargo that is handled in the Port is valued at over $150 billion and serves 80 million people, or 35 percent of the entire U.S. population. In 2005, the Port handled over 5,500 ship calls, 86 million tons of general cargo, 852,297 autos, and 2.9 million containers, approximately 8,200 containers each day. Today, international trade accounts for approximately thirty percent of the U.S. economy. Considering all this, it is easy to understand how a terrorist incident in one of our ports would have a devastating effect on our Nation and its economy.

Cargo Security

Standards and Procedures

America's consumer-driven market depends upon a very efficient logistics chain, of which the Nation's ports are a single link. U.S. ports provide the platform for the transfer of imported goods from ships to our national transportation system—primarily trucks and trains—that ultimately deliver those products to local retail outlets or raw goods to manufacturing plants. Historically, that goods movement system has had one overall objective: to move cargo from Point A to Point B as quickly, reliably and cheaply as possible. Today, a new imperative—national security—has been introduced into that system. The ports themselves are not the lone point of vulnerability. Rather, the potential for terrorist activity stretches from the cargo's overseas point of origin or place of manufacture to where the cargo is placed into a container to any point along the cargo's route to its ultimate destination.

Our goal should be to increase our level of confidence that we know exactly what is in each container *before* it is loaded on a ship destined for a U.S. port. It is simply not possible to physically examine the contents of each of the 8,200 containers that arrive each day in the Port of New York and New Jersey alone without seriously impacting the efficiency of the logistics chain. And we remain concerned about a requirement that 100 percent of all containers entering the country be scanned, before the technology, business processes and sovereignty issues have been addressed. The key, rather, is to identify a way to separate high-risk cargo from the vast majority of legitimate containers and then deal with the exceptions. This approach requires a thorough understanding of the existing logistics chain that moves containers from any place in the world to our Nation's distribution system.

A typical container movement includes 14 different nodes, involves 30 organizations, and generates as many as 30–40 different documents with over 200 data elements. This is a complex process in which the physical movement of a container is only one dimension of the system. There are three other important components that must also be understood: the flow of money, the flow of information concerning that shipment, and, finally, the transfer of accountability for the shipment, all of which must occur seamlessly in order for the cargo to be delivered to its final destination.

Today, no mandatory security standards apply when loading a container at the manufacturer or when it is consolidated in a warehouse, often well inland of a seaport. No security standards exist for the seals placed on containers. Cargo is transferred from one mode of conveyance to another and there are neither standards governing how that conveyance occurs, nor accountability for the integrity of the container as it changes hands.

We believe that efforts must be taken to verify the contents of containers before they are even loaded on a ship destined for a U.S. port. The process must include certification that the container is free of false compartments, and was packed in a secure environment and sealed so that its contents cannot be tampered with; that

there be an ability to verify along the route that neither the container nor cargo has been tampered with; that the container is transported under the control of responsible parties; and that the integrity of the information and information systems associated with the movement of the cargo has not been compromised.

We support Section 204 of SAFE Port, which requires "minimum standards and procedures for securing containers in transit to the United States." However, we also believe that we need to go one step further and make those container security standards *minimum and mandatory.* Voluntary cargo security measures such as those established under the Customs-Trade Partnership Against Terrorism (C–TPAT) program are helpful but are not sufficient by themselves in order to protect our homeland. Rather, all containers destined to the United States should be subject to a new and higher security standard. Then and only then, should importers that choose to go above and beyond the minimum standards reap tiered benefits such as those currently available through C–TPAT participation. The incentives to go above and beyond the minimum standards would be commensurate with the level of investment in and effectiveness of security measures and should include a number of security and commercial benefits including a reduction in cargo loss, fewer Customs exams, an adjustment to insurance premiums and bonding requirements and greater cargo visibility to support just-in-time inventory pressures. Those that don't meet the minimum standards would receive a "red lane."

The Department of Homeland Security is working on the development of functional requirements for Container Security Devices (CSD). Based on comments that Customs and Border Protection (CBP) Commissioner Ralph Basham made before the Center for Strategic and International Studies in July, it appears that the CSDs will be required only of Tier III C–TPAT participants. We are concerned that this approach only makes the secure shippers more secure and fails to address the vast majority of shippers that have chosen not to participate in the voluntary C–TPAT program.

The SAFE Port Act also required DHS to collect more data on cargo shipments before lading in order to improve their risk targeting. We support this advanced information effort, which is affectionately known as "10+2", and applaud CBP for collaborating with trade in the identification of the appropriate data elements and reporting methods. We join with our industry partners in eagerly anticipating the release of the Notice of Proposed Rule Making later this year. We are very concerned, however, about plans to develop a third party data warehouse or what is referred to as the "Global Trade Exchange" without appropriate consultation with industry and before the effectiveness of "10+2" can be evaluated. We respectfully request that through the Commercial Operators Advisory Committee (COAC) on which the Port Authority has a seat, that DHS involve industry in the development of the Global Trade Exchange concept, before any segment of it is developed outside the established consultative process.

Weapons of Mass Destruction—Radiation Detection

Radiation detection is yet another line of defense but radiation detection in the United States after cargo has arrived on our shores should be our last line of defense, not our first. We fully support the deployment of radiation detection equipment at the 22 highest volume ports in the country to scan all containers for radiation. However, as the technology is improved and resources allow, this program should be expanded beyond the highest volume ports. Not doing so would allow exploitation of the path of least resistance. In the Port of New York and New Jersey 98 percent of our import containers are currently scanned for radiation by CBP. Those that are not scanned today represent only the lowest risk containers that move inland by rail. We are monitoring the progress of the rail pilot project in the Port of Tacoma, which, if successful, will help us devise a solution for capturing that remaining 2 percent of rail cargo.

Starting in 2003, the Port Authority has worked closely with the Department of Homeland Security (DHS) on a Counter Measures Test Bed (CMTB) program at the New York Container Terminal to test and evaluate the performance of commercially available and advanced radiation detection equipment in real world situations. These efforts have led to the further development and selection of manufacturers for the Advanced Spectroscopic Portal (ASP) program. To date CBP has installed ASPs at two of our seven container terminals. Those ASPs are currently undergoing field-testing and have not been fully commissioned yet. CBP's cooperation in accommodating local operational constraints and schedules has been outstanding.

We recognize that concerns that have been raised by the Government Accountability Office, the National Resources Defense Council and others about the ability of the ASPs to detect shielded nuclear material and support the additional testing, evaluation and certification that is underway. If requested, the Port Authority will

continue to make its facilities and personnel available for any additional testing that may be necessary. Further, because of the limited ability of the ASPs to detect shielded material, we strongly support the Secure Freight Initiative, which integrates radiation detection and container imaging. We must continue urgently to pursue a solution that is easy to administer by the supply chain workforce; that is fast, accurate and reliable; and that is affordable.

Credentialing

In 2002, Congress mandated that all transportation system workers who are permitted "unescorted access" to restricted areas carry a Transportation Worker Identification Credential, or TWIC. TWIC is a tamper-resistant identification card with biometric capabilities that can be issued only after a successful criminal history background check. TWIC provides the operators of critical infrastructure with the ability to positively identify an individual seeking to gain access to a secure area. We fully support the need for positive access control at port facilities and the creation of a national identification program.

Since TWIC has been and will be the subject of several other hearings, I will limit my comments to just two issues relating to the SAFE Port Act.

The first is the provision requiring DHS to establish a pilot program to test TWIC card readers at five geographic locations in order to evaluate business processes, technology and operational impacts. While the SAFE Port Act mandated these pilot projects, the Department has not funded them. We and other port authorities and vessel operators are committed to assisting the Department in achieving its goals relative to the implementation and deployment of TWIC in the maritime industry. Accordingly, we have agreed to work with TSA to use our facilities and vessels, as well as use a portion of our Federal grant monies (FY 2006 and FY 2007), to test the equipment that will be used to read the TWIC cards. The Federal grant moneys, however, require a 25 percent cash match.

In order to devise a meaningful pilot project, considerable initial disruption will occur at each participating facility and vessel and both capital and operating funds will be expended that will not be recoverable at the end of the pilot, whether or not it is successful. We would suggest that the cost to the participants to plan, manage and implement this program already represents a significant contribution, even without an obligation for a cash match. Therefore, mandating a 25 percent cash match for purchase of infrastructure and equipment required for participation in the pilot project will place an undue burden on us, and will only serve to reduce the amount of resources we will have at our disposal to ensure that a complete implementation of TWIC is a success. We have therefore requested that Secretary Chertoff recognize the in-kind contribution that our organizations will be making and waive the cash match requirement pursuant to his authority under 46 U.S.C. 70107, section (c)(2)(b). We would appreciate the Committee's support of this request as well. All previous TWIC pilot projects were fully funded by the TSA, and the pilot project required under the SAFE Port Act should receive the same level of support.

The second issue is the prescreening of port truck drivers. Under Section 125, DHS was required to implement a threat assessment screening for all port truck drivers with access to secure areas of a port and who possess a commercial drivers license but not a hazardous materials endorsement. This program would be very similar to the interim screening program in which all facility owners and operators were required to participate in early 2006. Although this program hasn't been rolled out yet, we feel strongly that DHS comply with this requirement so that industry has a better understanding of what the impact of TWIC might be on the truck driver community. Current estimates indicate that anywhere from 10–40 percent of truck drivers may not be eligible for a TWIC, which could seriously impact port productivity and ultimately security.

Command and Control

In the President's National Strategy for Maritime Security, Maritime Domain Awareness (MDA) is defined as "an effective understanding of anything in the maritime environment that can affect the safety, security, economy, or environment of the United States." MDA is heavily dependent upon information fusion.

Additionally, one of the principal outcomes of the work of the 9/11 Commission was its determination that information sharing and collaboration at all levels of government are less than adequate. As such, we support the SAFE Port Act requirement for the development of interagency port security operations centers in key U.S. ports to facilitate operational coordination, information sharing, incident management and effective response. We would caution, however, that since the maritime industry does not operate in a vacuum but rather is largely dependent on surface transportation (road and rail) and requires the involvement of multiple levels of gov-

ernment and public safety agencies, these operations centers should not be limited to maritime and cargo security alone but be a single focal point and provide for the integration of all Homeland Security related functions among local, state and Federal agencies in a given region. It must also not just be a single operations center but one of multiple coordinating nodes in a regional and national information-sharing and collaboration network.

One of the cornerstones of effective maritime domain awareness and command and control is the Coast Guard's Command 21 program, which regrettably hasn't received sufficient funding and resources yet. Therefore in the Port of New York and New Jersey we applied for and received Federal funding to develop the concept of operations and functional requirements for what might become the Joint Port Operations Center in our Port. It is our hope that our work locally will help inform the development of national functional requirements under Command 21.

The basis for the local con ops and functional requirements will be the Port Authority's Joint Situational Awareness System (JSAS), formerly known as the Regional Information Joint Awareness Network or RIJAN. JSAS is a DHS-funded, DOD managed and Port Authority-led multi-agency project to build an information sharing and collaboration network among key operations centers in the New York and New Jersey port region. Regional partners include the States of New York and New Jersey and the City of New York. DHS sponsorship is via the Domestic Nuclear Detection Office (DNDO). Our DOD program manager and developer is the U.S. Army's Armament, Research, Development and Engineering Center from Fort Monmouth New Jersey.

Response and Recovery

While most of our focus since 9/11 has rightly been on preventing another terrorist attack, we must develop comprehensive programs to address response and recovery as well.

Recovery and Economic Impact

A large-scale terrorist attack at a Port such as ours would not only cause local death and destruction, but could paralyze maritime commerce and economies nationally and globally. Before such an event occurs, we must have plans in place to ensure an efficient and effective response in order to avoid critical delays in recovery and expedite business resumption. Agencies in the Port of New York and New Jersey know better than anywhere else in the country how to respond to suspected terrorist activities and catastrophic events. What is not entirely clear is how private sector resources could be leveraged to strengthen the response, what the economic impact of a protracted port closure would be, and how the private sector would be kept informed to facilitate critical business decisions as an event unfolds. We must collaborate today on developing localized plans and procedures to ensure a timely and effective recovery from an incident at our Ports and to inform the private sector as an incident develops and response and recovery takes place.

The Strategy to Enhance International Supply Chain Security, released by DHS in July, does a credible job of outlining the plan and considerations for resumption of trade. However, those considerations still need to be translated into port specific recovery and trade resumption plans.

Through the Area Maritime Security Committee, the Port of New York and New Jersey has developed a draft port recovery plan. We have also established a Recovery Advisory Unit to counsel the Captain of the Port and Unified Command on the priorities, requirements and limitations for an effective and efficient recovery. We await the release of a Navigation and Vessel Inspection Circular later this year, which will provide the necessary guidance to local Coast Guard Sectors for the development of port specific recovery plans. A crucial element however, before we can finalize our port recovery plan is the release of both CBP and USCG's tactical plans for recovery and resumption of trade, which hasn't been done yet.

The SAFE Port Act creates a prioritization for reestablishing the flow of commerce in the aftermath of an incident. We applaud the Department for recognizing that a port's ability to re-establish the flow of commerce will be incident-dependent and be dictated by ongoing response or clean up activities, current threat information and the availability of transportation infrastructure and resources (pilots, tugs, rail cars, barges, labor, cranes, tankage, container storage, etc.). Local port officials must have maximum flexibility to respond to their specific circumstances according to the dictates of the immediate situation. The recovery plan for New York and New Jersey makes life safety and public health, such as home heating oil in the winter, a priority; thereafter, vessels will move on a first-in, first-out basis depending on the availability of infrastructure and resources.

Research and Development

Today, cargo security projects are being managed by various agencies within DHS as well as DOT, DOD and DOE. There are also a number of private-sector cargo security initiatives. From our vantage point, little coordination and collaboration takes place among these various initiatives. As a result, we may be expending scarce research resources in duplicative efforts or pursuing technologies or devices in one program that have already been shown to be ineffectual in others. We risk reinventing the wheel in developing solutions already addressed and solved in other efforts. Erecting administrative barriers between these programs impedes the free exchange of information that could otherwise promote efficiency and effectiveness in improving security.

For these reasons, we believe it is absolutely critical to coordinate all cargo security research and development efforts through a single office. We believe that office should be the Director of Cargo Security Policy, created under the SAFE Port Act.

There is an old saying that ignorance is bliss. In the current context, however, ignorance is an obstacle. Improving our national security is not a competition between government contestants seeking to conceal information in order to gain an advantage over other contestants. Rather, individuals involved in these efforts should be players on the same team working for the common good. In addition to project coordination through the Director of Cargo Security Policy, we would encourage the development of a Joint Program Office and a cargo security working group that includes private sector participation.

We also support the development of a DHS Center of Excellence (COE) for maritime security and domain awareness by the Science and Technology Directorate. This COE's research will help DHS facilitate and defend maritime commerce and global supply chains, minimize damage and expedite recovery from attacks or catastrophic events impacting maritime interests, and protect coastal population centers and critical infrastructure through the COE. DHS also seeks maritime security research that will integrate public and private resources and expertise into a coordinated effort to address maritime threats systematically; align Federal, state, local, foreign government, and private sector security efforts and activities; and support global maritime awareness and security. The Port Authority is a member of Government and Industry Advisory Committee for a proposal that has been submitted for the COE on Maritime Security. A field visit is scheduled for next week and we expect to learn about an award before the end of the year.

Funding and Resources

Port Security Costs

Before September 11, 2001, port security was primarily focused on cargo theft and smuggling; it has since taken on new meaning and urgency. However, there is an ongoing debate over whether port security is primarily a Federal Government or private sector responsibility. While that debate continues, the Port Authority and private terminal operators throughout the country have voluntarily taken significant steps to protect our seaports from the terrorism threat, because the consequences of not doing so are grave. Since the September 11 terrorist attacks, ports such as ours have instituted heightened security measures and spent substantial resources to increase security, both with capital improvements and additional security and law enforcement personnel. However, for every dollar that is spent on security, there is one fewer dollar available for the capital infrastructure necessary to accommodate the increasing volume of cargo our ports are expected to handle.

By the end of this year, the Port Authority will have spent over $100 million on port security costs since the September 11 terrorist attacks. While 30 percent of the total—about $30 million—has been spent on infrastructure improvements and security systems, the vast majority of our expenses are the result of a significant increase in the operational costs associated with maritime security. It is estimated that the annual operations and maintenance costs associated with the new security systems is on the order of magnitude of fifteen to twenty percent of the purchase price. Additionally, ports and terminals have spent significant sums of money on personnel costs, including the hiring of new security officers, overtime, upgrading security forces to use more professional services, and providing extra training. The Port Authority's port security operating costs have doubled since 9/11. This does not include the extra police required at all Port Authority facilities every time the threat level increases, which amounts to approximately $500,000 per week.

Port Security Grants

Since June 2002, approximately $1.3 billion has been made available under the Port Security Grant Program to port and terminal operators and state and local law enforcement and emergency responders. About 12 percent or $104 million of the

total has been awarded to entities in the Port of New York and New Jersey, arguably the highest risk port in the country. The Port Authority has received $25 million of that share.

The vast majority of the $1.3 billion in port security grants has been allocated to critical security projects for individual terminals and vessels. Since all U.S. port terminals and vessels are now compliant with the Maritime Transportation Security Act, we must shift our attention from "my" security needs to "our" security needs. We therefore support the provision to make grants available to address port-wide vulnerabilities identified in the Area Maritime Security Plans. Under the Fiscal Year 2007 Supplemental Port Security Grant Program, FEMA is requiring all Tier I and II ports to develop a 5-Year Port Wide Strategic Risk Management Plan, which will form the basis for future grant funding requests. We would like to see this requirement extended to Tier III and IV ports, to ensure that all Federal port security funding is distributed based on risk and in a coordinated fashion. The Port of New York and New Jersey has already developed a Port-Wide Strategic Risk Management Plan and is prepared to help other ports create theirs.

Port Security User Fee

Physical, technological, personnel and law enforcement enhancements at port facilities, many of which were mandated by new Federal regulations, have created a financial drain on the operators that run them. During its initial rulemaking process for the port security grants, it appears that the Federal Government grossly underestimated the operating costs for security. These security operating costs have not been eligible for port security grants and, as a result, have become unfunded mandates that industry has had to bear. Thus, while the Federal Government has provided $1.3 billion in port security grants over the past 5 years, this represents only a small fraction of the security costs that the industry has incurred over that same period.

In the absence of a consistent stream of Federal funding for port and cargo security, many ports around the Nation have been forced to impose customer fees to cover federally mandated port security expenses. While the Federal Government has implemented standard regulations, there is no uniformity or consistency of user fees. The general concern reverberating throughout the maritime industry is that this haphazard approach to fee implementation could put U.S. seaports at a serious disadvantage in relation to ports in Canada and Mexico.

Together with a shift in supply chain security measures from our Nation's ports to those abroad, we believe the expenses associated with the implementation of a more secure goods movement delivery system should be offset by the reallocation of revenue from the various user fees already collected from the maritime industry. We eagerly await the report on user fees that was required under the 9/11 Commission Bill. To supplement any shortfalls, the Federal Government should adopt legislation establishing a uniform, nationwide Port Security User Fee to help offset growing port security costs and resources for our Federal partners. In all cases, the revenues generated through such a fee should be dispersed according to a risk-based formula.

Federal Staffing and Resources

Clearly the responsibilities of both the Coast Guard and Customs and Border Protection (CBP) staff have increased exponentially in the wake of 9/11. Unfortunately, the level of resources and personnel needed to support this awesome responsibility has not grown at a commensurate rate. It is widely believed that the advent of technology reduces our reliance on personnel. To the contrary, technology does not eliminate the need for personnel but rather requires additional personnel for intervention and resolution of alarms or concerns generated by the technology. In the Port of New York and New Jersey alone, CBP needs approximately 10 percent more staff to conduct its port security missions. In FY08 our local CBP staffing levels are actually being reduced. The problem is even more acute on the aviation side, which I am also concerned about. One area of the Coast Guard's mission is operating at a 1996 staffing level despite a 139 percent increase in volume of activity. Left unaddressed, these staffing limitations will adversely impact the free flow of commerce, safety and security.

Conclusion

Addressing the issue of port and maritime security is an enormous challenge given the complexity of the international transportation network. Devising a system that enhances our national security while allowing the continued free flow of legitimate cargo through our ports cannot be accomplished through a single piece of legislation, or by a single nation. It requires a comprehensive approach with coordination across state and national lines and among agencies at all levels of government as

well as the cooperation of the private and public sectors and the international community. It also requires that we periodically step back, measure our performance and identify areas requiring improvement, be it through new legislation, executive regulations or programmatic changes.

I hope my comments today have provided you with some helpful insight into this complex matter. The Port Authority of New York and New Jersey is prepared to offer any additional assistance that you may require. Thank you.

Senator LAUTENBERG. Thank you, Mr. Coscia. Ms. Fanguy, it was interesting to see your card display. Has it been tested in any kind of a reader?

Ms. FANGUY. Yes. In fact, we've done testing on multiple levels. We have contracted—contractors review their testing. We've done independent testing and we've also tested some of our cards with the National Institute of Standards and Technology to ensure the cards work as expected.

Senator LAUTENBERG. All right. Well, I note with interest your announcement yesterday that TSA intends to begin TWIC enrollment in Wilmington, Delaware on October 16 or October 15, I wasn't sure and the next 11 locations soon thereafter. Why is TSA skipping over the Port of New York and New Jersey, the largest port on the East Coast and which the FBI has identified as the most dangerous two miles for terrorism in the country? Doesn't that get attention that says maybe we ought to be looking there, to do as good a job as we can?

Ms. FANGUY. We absolutely plan on doing a very good job with the Port Authority of New York and New Jersey. They are part of our overall plan and when we look at it, every port is extremely crucial to national security. In our overall deployment plan, we've developed a risk-based approach that balances security risk with program risk. So we've laid out the first 12 ports but as we get started at those ports, we will be announcing plans and I can tell you that the Port Authority of New York and New Jersey is coming shortly after these first 12 but we want to get it right at those first 12 before we move on.

Senator LAUTENBERG. Well, we hope you get it right at all of them but the magnitude of exposure in the Port of New York and New Jersey is one that we think deserves particular attention and if there is a fire burning, the fire is biggest right now in that area, identified by the FBI. So it doesn't really ring a good note for me when I hear that after the first 11 are done. How many TWIC cards have been issued and activated as of today?

Ms. FANGUY. In terms of Phase IV, which is the phase that we're in now, for the national deployment, we've begun enrolling our trusted agents and government personnel. So we're in the initial phases of rolling out those cards. But once we get to Wilmington, there will be 5,000 people approximately but we certainly anticipate in the next year that we'll be enrolling probably close to a million workers.

Senator LAUTENBERG. How many card readers are in place?

Ms. FANGUY. The card readers are the responsibility of local port facilities.

Senator LAUTENBERG. No, how many are in place, Ms. Fanguy?

Ms. FANGUY. I would need to get back to you on what current port facility owners and operators have within their own physical infrastructure.

Senator LAUTENBERG. It's my understanding that ports that are testing the new TWIC card readers as part of the TSA pilot program and they are being required to use their port security grant funds to do so and must pay, as we heard, 25 percent of the cost. Now, TSA could eventually decide that the technology is unacceptable and the port then, would be stuck with useless equipment and so, why shouldn't TSA pay for the entire amount of testing?

Ms. FANGUY. We received the letter that was addressed to Secretary Chertoff and we are analyzing the letter as we speak. The current approach is to leverage the port security grant program and to implement technology that would be used for the long-term, once the Coast Guard puts out the rule that would require readers.

Senator LAUTENBERG. Would you recommend that TSA—that the various ports are relieved of a 25 percent commitment to the program for the reasons I stated?

Ms. FANGUY. I think it warrants further analysis and that's what we're doing right now.

Senator LAUTENBERG. Mr. Coscia, from an industry perspective, what—you talked about response and recovery after a security incident. Obviously then, you're challenging whether or not current plans for resumption of trade are adequate.

Mr. COSCIA. Senator, I think we've all come to recognize that in the event of any incident, there is a high degree of likelihood that even greater damage would occur by our inability to recover from whatever occurred and when you look at the criticality of the Port of New York and New Jersey, not just to the regional economy in New York City but frankly, to the national economy, its inability to operate efficiently or reactivate itself quickly would have an enormous national economic impact. We think people have come to understand that and as they develop plans to respond to an incident, we believe that there is a separation between the plans being developed at the Federal level, at the local level and more importantly, industry, which comprises around 90 percent of that supply chain apparatus, is not necessarily being integrated and required to provide the same kind of post-incident recovery planning and that we believe, Senator, is fundamental to it being effective. It will do us no good to have government agencies know exactly how to respond after an incident if we're highly dependent on private sector parties who have developed independent plans in which we are not fully integrated.

Senator LAUTENBERG. Well, your AMSC had a task force that recommended the Federal Government collect a per container fee to be used for port security. Now I assume that this is only effective if it's collected at every port so that there is not a competitive advantage if one port doesn't comply.

Mr. COSCIA. Senator, in preparing for today's testimony, our staff compiled a listing of port security fees that are imposed by ports around the United States and without getting into that in any great detail, although we certainly can make that information available if your staff has not already compiled it, it shows you what the problem is, which is that each port is making an individual decision about how much they are looking to assess on traffic coming through their facility. They are making that judgment by trying to balance their various cost issues and provide security

that they think is adequate and in doing that, they have to worry about whether or not in so doing, they've made their port uncompetitive and simply going to divert port cargo to another U.S. port. We think that a national policy on a port user fee, at a minimum, would provide a certain amount of uniformity to it so that these decisions can be based on security risk and not some balancing of competition among U.S. ports, which we think is totally inappropriate.

Senator LAUTENBERG. Thanks, Mr. Coscia. Senator Stevens?

Senator STEVENS. Thank you very much, Mr. Chairman. Admiral, the basic law of the SAFE Port Act requires the Coast Guard to reassess security measures at foreign ports every 3 years. How many ports do you assess?

Admiral PEKOSKE. Senator, we assess 138 ports. We have completed 109 already, roughly 80 percent and we're resourced to——

Senator STEVENS. How long did that take?

Admiral PEKOSKE. That took about a year, sir and we're resourced to revisit those ports at least every 2 years, which is in excess of the requirements of the SAFE Port Act. There's another element of this, sir, that I'd like to mention and that is that as we visit ports and as we engage internationally, there is a very big training component of this because as was mentioned before, some of these countries don't have the resources that we have here to develop a security system.

Senator STEVENS. Well, I'm interested, Admiral, in the allocation of cost to that compared to the allocation of cost of protecting our shores, our fisheries. There seems to me that a lot of the money that the Coast Guard has is being siphoned off now on the overall security process. Would you agree with that?

Admiral PEKOSKE. Sir, fisheries enforcement is also a security mission. Our presence in the fishery grounds provides a security presence for the United States.

Senator STEVENS. Well how then, do you have one-third of the boats you used to have before 9/11, in Alaska waters?

Admiral PEKOSKE. One-third the boats we had before?

Senator STEVENS. We have one third of the boats we had before 9/11.

Admiral PEKOSKE. Yes, sir. Well, as you know, we're in the beginning stages of our Deepwater Project and our patrol boat fleet is reduced from what it was before. We're working very hard to close those gaps as quickly as we can but it is part of an acquisition process that is taking us some time.

Senator STEVENS. We have, as I said, our Port of Anchorage has 90 percent of the goods that comes in through that one port. It doesn't seem to be very high on the pecking order as far as the Coast Guard is concerned. Why is that?

Admiral PEKOSKE. Sir, it is high on the pecking order. In fact, we have one of our Maritime Safety and Security teams in Anchorage.

Senator STEVENS. You do have a team there, yes. They are a small team. I've visited it and it's very nice.

Admiral PEKOSKE. Yes, sir.

Senator STEVENS. But in terms of inspection services, how often do you inspect U.S. ports?

Admiral PEKOSKE. We inspect U.S. facilities twice a year, sir. We have a scheduled inspection and an unannounced inspection and that has—that meets the requirements of the SAFE Port Act. I would also note that we have the ability, if there is an incident, to flow resources to whatever port needs that response and that's part of our Deployable Operations Group Operation, which we just began on the 20th of July.

Senator STEVENS. I don't know of any other state that depends on one port as much as we do. Our state is one-fifth the size of the United States, and all the goods that come in by water come into one port.

Admiral PEKOSKE. Yes, sir.

Senator STEVENS. I really do not think we have the protection that's needed and on the other hand, I think that we're losing protection for other resources, such as fisheries. Mr. Winkowski, what do you think about this mandating 100 percent screening? I've always believed that 100 percent is almost impossible in any situation but we are now looking at a 100 percent screening requirement. What's your approach on that?

Mr. WINKOWSKI. Well, it's certainly, Senator, going to be a challenge. I think the good news here, though, is that we have a lot of experience in pushing our borders out. Customs and Border Protection developed that program. It started—our first port was in Vancouver in February 2002. So under the CSI program, we have learned a lot. Now we're in 58 locations, accounting for 85 percent of the cargo that's coming into the United States. To add to that, Senator, the upcoming test that I talked about——

Senator STEVENS. Well, let me ask you this. What about this voluntary Customs-Trade Partnership Against Terrorism Program? Is that working?

Mr. WINKOWSKI. Yes, it is. It is working very well.

Senator STEVENS. Has the industry invested much into it?

Mr. WINKOWSKI. Oh, yes. The industry has invested a tremendous amount.

Senator STEVENS. Could you give us a little statement for the record on that?

Mr. WINKOWSKI. Yes. The——

Senator STEVENS. Not now. I mean, just provide one for the record.

Mr. WINKOWSKI. Sure, OK.

Senator STEVENS. I'm almost out of my time, as a matter of fact. I would like to ask Ms. Fanguy about these cards. You say that you think the people involved will pay how much?

Ms. FANGUY. Each card is $132.50—$132.50.

Senator STEVENS. Is that for a permanent card?

Ms. FANGUY. That's for a five-year card for someone who has not had a comparable security threat assessment conducted.

Senator STEVENS. What about those who have been involved before?

Ms. FANGUY. For people who have a comparable security—a reissuance would be again, the same, $132.50 because we re-run all of the same——

Senator STEVENS. Every 5 years?

Ms. FANGUY. That's correct.

Senator STEVENS. Does that repay the cost of those cards?

Ms. FANGUY. Yes. The program is fully fee-funded and so once we begin collecting fees, we will not require any more appropriation.

Senator STEVENS. You said you estimated there would be a million people who will have them within the next year?

Ms. FANGUY. Approximately.

Senator STEVENS. What percentage is that of the total required?

Ms. FANGUY. We would plan in the next year to enroll everyone who requires unescorted access to the Nation's ports and vessels. However, there is a lot of turnover in this industry. We're very aware of that and so we know that after this initial enrollment, that we need to be able to sustain ongoing enrollment for new workers or for people who perhaps changed jobs within the maritime industry and then would require unescorted access in the future. So we see this as a long-term operation and we need to make sure that we have things right in this initial enrollment but also for the long-term.

Senator STEVENS. One more question. How close are we to 100 percent inspection? Mr. Winkowski?

Mr. WINKOWSKI. We are testing this month, three locations in Pakistan, the United Kingdom and in Honduras, 100 percent scanning.

Senator STEVENS. That's overseas.

Mr. WINKOWSKI. That's overseas, yes. We have a report due up here in February and April and we will take those best practices——

Senator STEVENS. Doesn't that 100 percent apply to domestic ports, too?

Mr. WINKOWSKI. Well, this is under the Secure Freight Initiative, taking on three ports for 100 percent scanning of cargo that's coming to the United States. So all the scanning would be done overseas prior to it coming into the United States.

Senator STEVENS. You won't be doing any inspection in U.S. ports?

Mr. WINKOWSKI. Oh, no. We still can—that can still be subject to inspection.

Senator STEVENS. Well, I've been to the major ports on the West Coast. They're not near 100 percent. How soon will they be 100 percent?

Mr. WINKOWSKI. Well——

Senator STEVENS. Is that obtainable, is what I'm saying.

Mr. WINKOWSKI. When you look at seaports, we're going to be at 98 percent screening of our RPMs—Radiation Portal Monitors at the end of this calendar year.

Senator STEVENS. That's actual screening or selective screening?

Mr. WINKOWSKI. It's actual screening where every container will go through a radiation portal monitor, 98 percent of the containers will have gone through it.

Senator STEVENS. This year?

Mr. WINKOWSKI. At the end of this year, yes sir.

Senator STEVENS. 2007?

Mr. WINKOWSKI. Yes.

Senator STEVENS. Thank you.

Senator LAUTENBERG. Senator Cantwell, your questions, please.

Senator CANTWELL. Thank you, Mr. Chairman. I just wondered, from a broad perspective, if you could give us a grade as a Nation on where we are with port security? I'm not asking where we are with the resources we have or the implementation of SAFE Port or C–TPAT or any of the TWIC—I'm just asking where we are versus the goal of making sure that we have a redundant security system. What grade would you give us, the United States in where we need to be? Each of you could just——

Admiral PEKOSKE. Senator, I would give us a grade of a B. I think we have some of the fundamentals securely in place. We know the direction we need to go in. The challenge is just getting to the end point but I think we're at a B right now. I would say we were probably at a C last year. So just in the past year, we've made some progress.

Senator CANTWELL. Why do you think we've gone from a C to a B?

Admiral PEKOSKE. Because we have done a much better job on our International Port Security Liaison Officer Program, where we inspect and assess international ports. We have continued to gain knowledge as to how to integrate operations at the port level. That has been very successful. We've done a lot of work at looking at the small vessel threat and how we would close that threat gap. So there has been a lot of progress, just fundamental to providing good port security overall.

Senator CANTWELL. Can the rest of the panel answer that?

Ms. FANGUY. I would agree and I feel like we're turning upward. We're working closely with our partners within DHS and trying to continue to look for areas of improvement.

Mr. WINKOWSKI. I'm going to step out here a little bit, Senator and give us a B+. I really think that we have come a long way since 9/11 in Customs and Border Protection as a department in this whole area of screening and scanning cargo, advance information, pushing our borders out.

Mr. CALDWELL. I'm going to give an incomplete. One of the frustrations for us as well as Congress, is the lack of performance metrics to measure a lot of these programs. In a lot of cases, the lack of metrics is one of the main weaknesses that we have. It's very difficult. How do you measure security? It's easy to talk about but measuring it is pretty hard.

Mr. COSCIA. Senator, from the industry's perspective, I would say if the first day of school was September 12, for some reason, we didn't show up at school at all for some period of time. And then we finally woke up and realized we needed to. I think since then, a lot of progress has been made. The agencies represented by the others who are here today, I've seen some real promise for encouragement. But I do think we have a long way to go at recognizing just how comprehensive this issue is. So I'm afraid I can't do much better than a C but I hold us all essentially responsible for that grade.

Senator CANTWELL. I thank you for that answer and I think I agree with you and Mr. Caldwell. I wasn't asking about necessary performance although I do think there have been some issues about implementation and performance and measurements, as Mr.

Caldwell said. But I'd find it hard to give us better than a C, given the threat and the challenge that we face and I think we're always going to be short on resources. Our resources are going to be dear so making sure they're deployed in a cost-effective manner is going to be of importance. I want to get back to Admiral Pekoske about this. Well, Mr. Coscia, you mentioned—well, I think most of you mentioned this international issue and where we are and the challenge. Mr. Caldwell, you mentioned the smaller ports not having regimes on an international basis. So how do we feel secure if you're thinking about an entire worldwide infrastructure and as I said, when we have thousands of cargo containers coming in every day to our ports, this is a real concern, the fact that there might—so you're saying we have—I can't remember what percentage you said—of how many ports on an international basis had been protected but we still have this web and you're saying, well, let's do every 2 years checking the system.

To me, we should be much more aggressive on the IMO—International Maritime Organization, of getting everybody to agree to a security regime and then having the security regime checked on a consistent basis. So why can't we move toward that so that we're upping our numbers of cargo containers checked? Because obviously, we already are well aware that terrorists go at the weakest point in a link. That's their assessment. They don't say, "oh well, we know that Asia's got its act together on safe ports so we're going to go over here instead." I mean, how do we get this regime into better shape?

Admiral PEKOSKE. Senator, we have an international regime, a global regime right now called the International Port and Facility Security Code and when we make foreign port assessments, we're basically assessing a country's performance against that global code.

Senator CANTWELL. But we were just hearing from panelists about that voluntary system. So what I'm saying is, if we want to get better than a C or incomplete, which I think we want to, don't we have to come up with a better system?

Admiral PEKOSKE. The system is not entirely voluntary. If countries agree to the code and if they don't comply with the code, then there are conditions of entry that we place on them that has an economic impact on their ability to conduct business in this country. And we've already seen countries improve their security profile as a result of that incentive. And Senator, we're over at IMO right now, the Maritime Safety Committee is meeting in Copenhagen over the next 2 weeks.

One of the things they're talking about is the implementation of the long-range tracking system, which is a global tracking system. It will give us, for the very first time, visibility—as soon as a ship declares, no matter where it is on the globe that is heading to the United States, we'll be able to track that ship on its voyage over. We'll also be able to see every ship that's 1,000 miles off our coast and that's a very significant improvement in capability. And if I could, I would like to make just one other point. It's been raised a couple of times this morning. We are revising our port security assessment model to go to a risk assessment model. We want to base our decisions, our funding allocations, our activity levels, on

risk and we've got a very good maritime security risk assessment model in place. We've deployed it to each one of our Captains of the Port and that's how they're designing not just their response plans but also their recovery plans and those recovery plans, I couldn't agree with Mr. Coscia more, the key part of these recovery plans has to be the private sector and we fully agree with that and that will be part of the process that as we develop these individual, port-specific plans, the private sector will be a key part of it.

Senator CANTWELL. I appreciate that but I would say, I don't think someone wanting to do harm to the United States cares whether a cargo container sits in the red lane or not, as long as it makes it here, right? So the question is how do you get these other countries to participate in a security regime and I think—I personally believe we need to up this effort. But I want to turn to Ms. Fanguy because we're in the implementation stages of TWIC, I believe, at the Port of Tacoma, is that correct?

Ms. FANGUY. That is correct. It will be coming in November.

Senator CANTWELL. And we're a very integrated port system so we have workers from both the Port of Seattle and the Port of Tacoma. So they don't always work at the same spot. They don't always work at the same place so how are—I mean, I'm concerned that the—how the TWIC cards are being implemented if they're not being implemented on a regional basis. How is that security regime going to work when you have people working all around—maybe not even just the Port of Seattle and Port of Tacoma. We have the Port of Everett, the Port of Vancouver, because obviously people are employed where they're needed.

Ms. FANGUY. Compliance will be enforced at the regional level by the Captain of Port sector and so what we're really announcing now is opening the doors of a service center where you can go and get your TWIC. The center in Tacoma will be one of many in your area. But before we actually begin to work with the Coast Guard to determine when compliance will be enforced, all of the centers will be open and we're trying to make it as convenient as possible by opening 147 fixed enrollment centers so that people can go get their card at a place that's most convenient to them. In addition, we're also working with local stakeholders to identify opportunities to take TWIC to them. So as an example, by taking a mobile enrollment station to a union hall or to a major employer, again, so that we can make sure that we get full coverage in this initial enrollment period. So Tacoma is really just the first of many in your area and all across the Nation.

Senator CANTWELL. So you're saying they're going to be deployed but not implemented until the rest of the region is implemented?

Ms. FANGUY. Before we can actually enforce having the TWIC, we need to make sure that everybody has an opportunity to get a TWIC. So this is where we're trying to make it convenient to workers so that they have plenty of opportunity to apply but then when enforcement is brought in, everyone in the region would have had an opportunity to apply.

Senator CANTWELL. I know I'm over my time, Mr. Chairman but I wanted to say we want to continue to work very aggressively on this because I think there are—I think the contractor has failed to realize that there are multiple shifts, that there are workers that

are needed—that need access to the secure areas. There are a variety of different people who read power meters, who collect garbage, work at the various—work in a variety of entities and so I think all of this integration and as I said, we have truckers who make deliveries to different ports.

So, they're not necessarily just at the Port of Tacoma so how all that integration system works and obviously the TWIC Program in and of itself and its challenges. So we want to make sure that those concerns at the local level are being heard and that we're having a dialogue about them because we do want an implementation that works thoroughly. Thank you, Mr. Chairman.

Senator LAUTENBERG. Senator Carper?

STATEMENT OF HON. THOMAS R. CARPER, U.S. SENATOR FROM DELAWARE

Senator CARPER. Thank you, sir. To our panelists, welcome and thank you for joining us today. I want to make sure I pronounce everyone's name right. Ms. Fanguy?

Ms. FANGUY. Yes.

Senator CARPER. Has your name ever been mispronounced?

[Laughter.]

Ms. FANGUY. I'd say nearly 100 percent of the time.

Senator CARPER. But not by me. Huh? All right. Thanks, that's good staff work, keep me out of trouble. Welcome all of you and let me just ask a question of two of you, if I can. I'm from Delaware and in our state is the Port of Wilmington, the top banana port on the East Coast, we're proud to say. We've got a lot of people who work there and a lot of, particularly, produce is handled there as well as cars, inbound and outbound, auto exports. We've been focused a fair amount on the TWIC program in our state and at our port, as a lot of places have and I'm pleased to hear that the TWIC program is finally beginning at the Port of Wilmington and that the workers there can start enrolling in the program, I think, next week. October 16, whenever that is. Let me just ask how long you expect this first enrollment period to last before you begin enforcement at the port? How much notice do you expect to be able to provide to workers and to us, before you start enforcement? And a third part is how long will you test your initial operation before expanding it to other ports? So there are three questions and if somebody else wants to take a shot at this, you're welcome to as well. But again, three questions. How long do you expect this first enrollment period to last before you begin enforcement at the port? The second question, how much notice will you provide to workers and to us before you begin that enforcement and finally, how long will you test for initial operation before expanding to other ports? Including someone across the river in New Jersey?

Ms. FANGUY. Sure, absolutely. So again, going back to the concept that compliance and enforcement comes in by Captain of the Port zone, Sector Delaware Bay has quite a broad span and we're going to have quite a number of enrollment centers there, so the Wilmington, Delaware facility will be the first in that area as well as in the Nation.

Senator CARPER. Yes, but we have a motto in our state. We were the first state to ratify the constitution and our state motto is, "it's

good to be first." I'm quick to point out there are some things you don't want to be first at.

Ms. FANGUY. In terms of enrollment, we will be there for a significant period of time. I would say for the initial enrollment, months. But again, we like to think about this as a long-term activity so there will be a presence in all of the ports for the long-term, not just in this initial enrollment period. So when we talk about how long enrollment takes, what we're really trying to develop is a sustainable model to be able to have the right hours of operation, the right number of workers there to be able to take the people's information. In some places, we have 24/7 ports and in those places, we may do 24/7 enrollment. We want to work really closely with the local stakeholders to determine what makes the most sense. So we were actually in Wilmington, Delaware last week, meeting with the Port Director and his staff and starting to work more closely about what's going to make the most sense. We've already been working with them but we need to continue to monitor how things go.

Senator CARPER. Let me interrupt. Let's just go back to my three questions.

Ms. FANGUY. It's going to be several months for the initial surge period of enrollment. With the resources that we're going to deploy, we could do everybody, if they all came in exactly evenly, in 5 weeks but we don't think that's going to happen. So we're going to be there for months.

Senator CARPER. For several months?

Ms. FANGUY. For several months. The Coast Guard, as it's stated in our regulation, must give 90 days notice before we begin to enforce the use of TWIC.

Senator CARPER. OK. Ninety days notice beyond what? October 16?

Ms. FANGUY. Prior to the start of compliance. So a notice would be published at some date in the future and that would be——

Senator CARPER. That starts a 90-day clock?

Ms. FANGUY. That starts a clock.

Senator CARPER. OK. All right, thank you.

Ms. FANGUY. And then the third part of your question is on expansion. Based on the test results that we've had today, we would expect that we're going to start in Wilmington, October 16. We're then going to proceed through the rest of October, see how things go and early November is when we would go on to Corpus Christi and again, so we're moving on to a second single port, monitoring how the progress goes there and then beginning to expand nationwide. So we've listed the first 12 ports today but after we see the results of operations there, we do have an aggressive plan to be able to roll out nationwide to cover all of the other ports in some order.

Senator CARPER. All right, thank you. A related question, if I could, just to follow up. And you may want to answer this for the record but any idea how many people have been assigned to take applications at the Port of Wilmington, to help workers through the process?

Ms. FANGUY. Again, the model that we're using is to use a number of part-time casual laborers but we look at it in terms of our

overall—across all of the people, the shifts and the equipment, how many weeks will it take to do enrollment? So in Wilmington, Delaware, again, if people came in exactly evenly and they were all lined up and had pre-enrolled, we could do the entire operation in 5 weeks with the current equipment. We're going to also send a extra surge and again, if everybody came in exactly smoothly—another 3 weeks.

Senator CARPER. You're calling this a surge?

Ms. FANGUY. A surge. Yes.

Senator CARPER. Part 2?

Ms. FANGUY. Yes.

Senator CARPER. Any idea how many workers you expect to enroll during this initial enrollment period?

Ms. FANGUY. Enrollments in Delaware, we expect it to be approximately 5,000 but if it's more, we're ready to handle the volume.

Senator CARPER. OK, good. That sort of answers my next question. If it turns out you need additional workers to get through this initial surge of applications, do you have the funding and capacity to hire and train additional people quickly?

Ms. FANGUY. Absolutely. We have a contract structure in place that is extremely flexible. We pay a flat rate per worker. There's no additional cost to workers or to the government if we need to bring on additional resources.

Senator CARPER. OK, thanks. But, Mr. Chairman, could I ask one last question, if I may, please? Thanks very much. I don't mean to be picking on you, Ms. Fanguy, but I'm glad you're here and able to answer these questions. As you know, many of the longshoremen have criminal records because that line of work is one of the only good paying jobs that are open to some people with criminal records. But we're not trying to weed out those kinds that rehabilitate themselves and earn an honest living, of people who have made a mistake in their lives and seeking to atone for their sins and we want to make sure they have a chance. Can you explain how you plan to differentiate between those say with terrorist ties and those with a criminal record who are trying to earn a living now?

And the second part is, can you also explain any waiver or appeals process that is open to those people that are denied a card? So there are two questions. Can you explain how they plan to differentiate between those with terrorist ties and those with criminal records who are trying to earn a living now and making a honest living now and second, can you explain to us any waiver or appeals process that is open to those folks who are going to be denied cards?

Ms. FANGUY. Absolutely. So the disqualifying crimes that we've listed in our final rule are based on the aviation model for identifying potential ties to terrorism but every case is weighed on its own merits. We have a series of multiple reviews to look at a person's individual case and their particular background. We're basing our model for doing those reviews on other successful programs at TSA, such as the Hazardous Materials Endorsement Program, where we vetted close to 700,000 people to date. We do anticipate that we will have some people who do fall within the parameters

of those disqualifiers and that's where we work very closely with them to give them two opportunities.

One is an appeal because in some cases, we may have incorrect information and if that's the case, we want to be able to disposition those as quickly as possible and make sure that the person gets their card and on the HazMat Program, we have processed over 10,000 appeals and 99 percent of them have been—we've discovered that we had incorrect information and we gave the person their endorsement.

In terms of a waiver, that's where a person may truly have a disqualifier in their past but we work with the person. We send them a waiver packet that provides them with some instructions on how to provide us with information and we ask that the person take advantage of the waiver process and let us know how they may not be a—have any ties to terrorism and don't pose a security threat. So there are people who may have something in their past but it's absolutely not our intent to keep people from going to work. We're trying to keep people with ties to terrorism out of the ports so we want to work closely with workers.

Senator CARPER. I understand. It's a difficult balancing act. Mr. Chairman, you've been terrific. Thank you and Ms. Fanguy, so have you. Thanks so much.

Senator LAUTENBERG. Now, we like our neighbors—as a matter of fact, we're very fond of the state but it's smaller than ours.

[Laughter.]

Senator CARPER. We're only the 49th largest state. But we were the first.

Senator LAUTENBERG. And I remind everybody that New Jersey was the state where the Bill of Rights was first signed. And we're pleased to have the distinguished Senator from Maine here, Senator Snowe.

STATEMENT OF HON. OLYMPIA J. SNOWE,
U.S. SENATOR FROM MAINE

Senator SNOWE. Thank you, thank you, Mr. Chairman, thank you for conducting this hearing today, which is obviously a critical issue to our Nation because port security remains our greatest terrorist vulnerability and I know that this Committee has held numerous hearings over the years to follow up and to explore the gaps in port security and measuring the progress that we've made and trying to identify ways in which we can build upon the effectiveness of those programs that are working but also to make sure that we do everything we can to aggressively pursue closing the remaining gaps and I know we've made progress. I know it's an identified mission and I appreciated the GAO's report because I think it does give us, I think, a snapshot of where we stand today and obviously, I'm deeply concerned that we haven't been able to implement the Transportation Worker Identification Credential program—I mean, that's certainly lagging and second, the implementation of standardized inspections and scanning of containers, which has also been very—is critical to port security. So I want to begin with you, Admiral Pekoske, on several of these issues.

Obviously, the GAO has said that the Coast Guard remains resource challenged in a number of areas, one of which, of course, is

on inspections as well and I would like to follow up with you to ask you exactly what is the status of the number of inspectors that you're currently training? I know in 2006, you had 82 inspectors. We provided an additional $15 million to help expedite the training. I gather that's lagging at this point and we had the double inspection requirement both for domestic inspections and international facilities. I understand that has really not been implemented to the extent that it should be in meeting our commitment for inspections, both domestically as well as with international ports. So can you tell us today exactly where the Coast Guard stands and the number of inspectors, too. How many are being trained? And three, on the inspections, how many inspections have been conducted and how many need to be conducted and how are you going to meet the commitment with the new requirements in the law?

Admiral PEKOSKE. Senator, thanks for the question and I'll answer it in two ways. I'll talk about our domestic inspections first, if that's OK and then I'll talk about our international inspections. Domestically, the SAFE Port Act requires us to do one regularly scheduled inspection of every facility. There are roughly 3,200 facilities and then one unannounced inspection. So the Act requires two inspections per year. We have roughly almost 400 inspectors to be able to do that. We appreciate the Congress's support of additional inspectors to bring us up to a higher level, an addition of about 90 inspectors over the past year. That inspection level is adequate to conduct the one announced, one unannounced inspection of all the MTSA facilities that the SAFE Port Act has. As an example, in 2007, with 3,200 facilities domestically, we've done over 7,200 inspections so we are well on pace to actually exceed the requirement in 2007, domestically. Internationally, we have a smaller cadre of international inspectors, under 100 people, roughly 80 people that travel to the foreign ports, the 140 foreign ports. Senator, they've already inspected 108 of those 140, so roughly 80 percent and they will have all 140 complete by March of 2008.

So I consider that to be good progress and they've come back with some very, very good results. We intend to actually exceed the requirements of the SAFE Port Act. The SAFE Port Act requires that we visit every country every 3 years. Senator, we plan to visit them every 2 years because particularly at the early stages, this is a global system and providing that presence and that recurring training and plus that assessment is very important for us. So inspection-wise, we're in reasonably good shape.

One of the things we're doing as well, Senator, is the Commandant had an opportunity to speak before the Propeller Club a couple weeks ago and he talked about our overall inspection program within the Coast Guard and he made a couple of important points. One is that we need to stabilize, internally for the Coast Guard, our inspection workforce, more so than we have in the past, so that the expertise that is developed stays in the inspection program. And we also need to increase the number of civilian employees we have in that inspection program so that the military rotation system doesn't cause the level of churn that it currently does. So we'll have more civilians, predominantly still military but—and

even with the military, we're going to try to manage the rotation process so that expertise stays resident.

Senator SNOWE. So you're comfortable with the number of inspectors that you currently have to meet the requirements, both domestically and internationally? You're saying 300 that are fully trained at this point?

Admiral PEKOSKE. Yes, ma'am.

Senator SNOWE. It would be interesting, Mr. Caldwell. I'd like to have you address this question as well because I know in GAO, you address that particular question in saying at GAO that the Coast Guard was resource challenged in meeting the requirement of training these inspectors. Are you comfortable with what Admiral Pekoske is now saying?

Mr. CALDWELL. Well, let me try to address both, the overseas first and the domestic second. In terms of the overseas, the Coast Guard's big problem is that this is a new program. So they trained these people to be inspectors to do this program and now they're all toward the end of their rotation. But once the program has been in place for a number of years, you'll have more people rotating in and out and people in place to share that expertise. It's not just an issue of training with overseas inspectors. You have to have the right kind of person. They have to be diplomatic and be able to deal in a foreign environment. Obviously language skills are very important there. I think the toughest nut to crack for the Coast Guard is getting over this hump of replacing almost their entire first class cadre of overseas inspectors.

In terms of the domestic program, they've trained a lot of people but a lot of them are no longer assigned to do inspections and sometimes people that are currently assigned as inspectors aren't doing inspections. They have other duties as assigned. These are legitimate duties in terms of looking at safety or environmental issues as opposed to security inspections. Regarding Admiral Pekoske's comment about hiring some civilian inspectors, I think that could go a long way by providing more stability within an office. Within an individual Coast Guard sector, it's good to have somebody who has been there a number of years to know that a particular facility has always been a problem. That inspector might know that unannounced is better than announced inspections. That inspector knows to show up on a Friday night because he went by there on a Friday night 2 years ago and the gate was wide open.

I think that the Coast Guard is pretty receptive to the recommendations we're about to make about its inspection program. We actually have an exit conference tomorrow with the Coast Guard where we'll talk about our potential recommendations and I think we're satisfied that progress is being made. The bigger issue we have is the MISLE data, which is how they track these inspections, hasn't been kept consistently by the inspectors. Without cleaning up the data, it's pretty hard for the Coast Guard to make an evaluation of how well the program is working. For example, they could compare the results of unannounced inspections to announced inspections. Currently, the Coast Guard just doesn't have the data to do that type of analysis right now.

Admiral PEKOSKE. Senator, if I could add to that, Mr. Caldwell makes some very good points and we have taken a look at following

up on the data that we collect from these inspections and to be able to do with it just what he stated. If I could make two other points. We just had all of our international port security liaison officers—those that do the international inspections, here in Washington for a week conference and we talked to them about consistency in their program, the approaches they make to countries, how to conduct the inspections and so this is a new program and it is getting off the ground. We're going to be very careful that we don't have everybody reporting in and then 2 years or 3 years later, everybody reporting out. We're going to manage that transition very carefully. If I could make one other point with respect to inspections, we've taken a very close look, as you know, over the past four or 5 months, with our marine safety—not the security but the safety inspections and we know that we do not have enough resources for those safety inspections. And that inspection capability, when you're looking at safety and security issues, goes hand in glove. So, to conduct the safety inspections we need, plus with the advancement of industry, we do need more resources for that.

Senator SNOWE. I appreciate that. Thank you, Mr. Chairman. I do have just one other question? On interagency operational centers, I understand that the Coast Guard does not yet have a single comprehensive plan. Can you address that because I think that is also very critical to get the coordination that is, I think, so essential across this country with respect to the various ports and how they are integrated.

Admiral PEKOSKE. Yes, Senator and you're exactly correct. What we have done since 9/11 is we have prototyped across the country in five different locations, how you would develop an integrated command and we've learned an awful lot of lessons from that. We have a project called Command 21, about a $260 million project that will begin that process of integrated command centers. It kind of does it from a couple of perspectives. It's additional sensors, additional information systems to integrate the sensors and then the facilities so that when we have an integrated command center, we have a command center where all of our port partners can be with us in the same location, if that's possible and if that makes operational sense in the port. In some ports, that doesn't make operational sense. An example would be the Port of New York and New Jersey, where we do need to have some redundancy of command centers, due to complexity and size of that port. But you're exactly right. This is a concern of ours and as we look at our sectors, this is a number one priority for us, is to get those integrated command centers.

Senator SNOWE. And do you need additional money for that? I mean, is it—I understand there has been $260 million applied.

Admiral PEKOSKE. No, Senator, we need $260 million. We have not had the money for that yet.

Senator SNOWE. You have not had money yet? So that is essential?

Admiral PEKOSKE. Yes, ma'am.

Senator SNOWE. OK. Thank you. Thank you, Mr. Chairman.

Senator LAUTENBERG. Thank you very much, Senator Snowe. I just want to check something with Mr. Winkowski that was in your statement, where you talk about this fiscal year CSI expanded to

eight additional ports, reached a milestone of 58 ports worldwide, 85 percent of the container traffic destined to the United States. Now, how is that screening done? Is it a paperwork screening, Mr. Winkowski?

Mr. WINKOWSKI. We have Automated Targeting Systems that are employed. That's targeting the cargo overseas as part of our redundancy systems. We have Radiation Portal Monitors overseas.

Senator LAUTENBERG. Have all of these containers been reviewed by a technological device that says what's in there?

Mr. WINKOWSKI. They have all been screened through our Automated Targeting System, yes.

Senator LAUTENBERG. But just to be sure. Now, how much of that has been screened by a device and how much of it has been screened as a result of paper inspections?

Mr. WINKOWSKI. You have several scenarios. You have the automated targeting system I just talked about. On those containers that present a high risk for us, they are then put through a Radiation Portal Monitor for scanning purposes.

Senator LAUTENBERG. So in order to get to that stage, so it's a paperwork review. How about intelligence help from other places? The Inspector General report of 2006, "Automated Targeting Systems," that talks about the sources of intelligence information, are you dependent on others supplying data to you in order to get to the radiation screening?

Mr. WINKOWSKI. We have very close working relationships with many of the agencies that are in that business, the Coast Guard and we have a system in place to review that.

Senator LAUTENBERG. So it's not 100 percent radioactive screening or whatever the process is?

Mr. WINKOWSKI. Not at all. Not at all the CSI ports, no.

Senator LAUTENBERG. No. OK. Mr. Coscia, I was interested in the statement about the cost of Federal—cost of equipment. TWIC cost was estimated to be between $575 million and $831 million. The cost for facility owners, this is Ms. Fanguy's—it's your statement, I believe and I'm reading from it, so the cost for facility owners is estimated to be between $580 million and $1.6 billion and I'm rounding off here. Now, Mr. Coscia, do we have any idea what it might cost in the Port of New York and New Jersey to pick up their share of the screening, the screening equipment that is necessary?

Mr. COSCIA. Senator, I don't know that we know that number with great precision but our best estimate is that would be somewhere in the neighborhood of $10 million.

Senator LAUTENBERG. Ten million dollars?

Mr. COSCIA. That's correct.

Senator LAUTENBERG. And that would be borne by the Port Authority?

Mr. COSCIA. By the Port Authority but let me be clear. That number and the accuracy of that number is impossible to determine at this stage precisely. That number is our allocated cost sharing on the implementation of the program from a technology standpoint, from infrastructure.

Senator LAUTENBERG. Is that the 25 percent?

Mr. COSCIA. That's the 25 percent, roughly, I believe, yes. Beyond that, we have significant costs associated with different operational changes that we need to do in order to implement the system. So that's in essence, our contribution to the TWIC implementation from a mechanical standpoint.

Senator LAUTENBERG. As all of you have seen, we've been generous in our time allocation so, in a kind of schizophrenic thing, I'm going to say the Chairman—Mr. Chairman, you've out-questioned your time. So we'll keep the record open and we'll submit questions to you or permit members of the Committee to submit questions and would ask for your prompt response and I thank each one of you for your excellent presentations today.

[Whereupon, at 11:33 a.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF VAYL S. OXFORD, DIRECTOR, DOMESTIC NUCLEAR DETECTION OFFICE, DEPARTMENT OF HOMELAND SECURITY

Introduction

Chairman Inouye, Vice Chairman Stevens, and distinguished Members of the Committee, as Director of the Domestic Nuclear Detection Office (DNDO), I would like to thank you for the opportunity to share the progress we have made in improving port and cargo security. Keeping our Nation's ports secure is a critical layer in protecting our citizens against nuclear terrorism.

One year ago, the President signed the SAFE Port Act, which formally authorized the establishment of the DNDO. This important piece of legislation also identified a number of goals and reporting requirements for our Department. It helped ensure that we have the right security strategies in place and that we maintain our momentum as we implement protective measures.

I am happy to share that DNDO is meeting the requirements outlined in the SAFE Port Act. We have submitted a number of reports to Congress due earlier this year (including our comprehensive strategy for the deployment of radiological and nuclear detection equipment) and we expect to meet the deadlines for those that remain. We also have made excellent progress in deploying radiation detection technology at our busiest ports resulting in the screening of 93 percent of all incoming seaborne cargo into the United States.

Port Security Strategy

Before I go into more detail about the progress we have made in regards to the SAFE Port Act, I would like to explain our strategy at DNDO for deploying detection technologies to our Ports of Entry (POEs). Eighteen months ago, only 37 percent of incoming seaborne containerized cargo was being scanned for radiological and nuclear threats. DNDO worked in partnership with our colleagues at Customs and Border Protection (CBP) to develop a joint radiation portal monitor (RPM) deployment strategy that incorporates an optimized mix of current- and next-generation technologies, balancing our need for better capability with a desire for increased coverage against the associated costs of each. This joint strategy is predicated on placing next-generation systems, like the Advanced Spectroscopic Portal (ASP), at the highest throughput ports, where reductions to secondary inspection rates will have the greatest benefit. Deployment of ASP systems will be dependent upon the Secretarial certification of the systems as required by the FY 2007 Homeland Security Appropriations Act (Pub. L. 109–295).

Our strategy up to now has prioritized deployment activities based on risk, vulnerability, or consequence, as influenced by major populations, industries, importance to the economy and supply chain, or military bases located nearby. We also consider prior records of illicit activities. Finally, we consider whether locations had upcoming port reconfiguration.

We have taken steps to prepare for additional deployments and are conducting site surveys, developing site designs, and starting negotiations to award construction contracts for each of the crossings. As a general practice, DNDO works with the port authority to proactively schedule construction to coincide with any other activities at the port. This helps prevent scheduling delays and expedites the deployment process overall.

Our priority remains to finish deploying RPMs to high volume seaports and land border crossings. However, our future plans are addressing the hundreds of smaller crossings that dot the Northern and Southern borders, including rail crossings. We will also begin scanning of international air cargo.

Status of Deployments

RPMs have been deployed to all of the Nation's 22 busiest seaports. We are currently scanning 93 percent of cargo coming through our seaports using 358 RPMs. Moreover, at select major seaports, exit scanning now covers 100 percent of all con-

tainers and vehicles. By the end of this calendar year, 98 percent of all containerized sea cargo entering into the United States at the 22 busiest ports will be scanned for radiological and nuclear threats.

It is also important to mention deployments to our land borders. There are 241 RPMs operating on the Northern border and 343 RPMs operating on the Southern border. This results in scanning 91 percent of containerized cargo coming across the Northern Border and 97 percent coming across the Southern. In addition, a total of 60 RPMs are deployed to sites such as mail and express courier consignment facilities. By focusing on major ports of entry first, we have been able to dramatically boost the scanning levels of incoming cargo. We are also conducting scanning of privately owned vehicles (POVs). Our detection equipment currently scans 81 percent of POV traffic coming across the Northern border and 92 percent across the Southern.

Meeting the Requirements of the SAFE Port Act

Based on the progress we have made with RPM deployments at POEs, we are meeting the mandates set forth in the SAFE Port Act that require that all containers entering high-volume ports by vessel be scanned for radiation. In addition, we have developed the required strategy for the deployment of radiation detection capabilities, and that strategy has been submitted for the record as an amendment to this testimony. However, there are a number of other requirements outlined in the Act that we have been asked to fulfill and I would like to give you an update on each.

In total, the SAFE Port Act outlines five reporting requirements for DNDO. Our deployment strategy was submitted first to Congress in March 2007 and included information on a risk-based prioritization of ports, a proposed timeline for deployment, the types of equipment that we are proposing for each port, documentation of standard operating procedures for examining containers, operator training plans, and the Department's policy of using non-intrusive imaging equipment. As I mentioned earlier, one aspect of our joint deployment plan with CBP is how we plan on introducing next-generation technologies like ASP into the field. Right now, ASP is pending Secretarial certification and will not be fully deployed until that certification process is complete. If the outcome of the certification process is positive, we will submit an amendment to our strategy to identify the locations at which we will deploy ASP. The report also included a classified annex that details plans for covert testing of the top 22 seaports, as required by Section 121 of the SAFE Port Act. The DNDO Red Team is working with CBP to build and maintain documentation of these activities.

Second, in April 2007, we submitted a joint report with the Science and Technology Directorate, CBP, and DHS Office of Policy Development that outlined the feasibility of and strategy for development of chemical, biological, radiological and nuclear (CBRN) detection equipment. DNDO submitted content that clearly documented both near- and long-term research and development efforts that will provide improved nuclear detection capabilities.

The third report required that DNDO, along with CBP, complete an evaluation of health and safety issues related to the use of non-intrusive imaging (NII) technology to scan containers. DHS fully understands the environmental health and safety impacts of NII technology. DHS has a comprehensive radiation risk reduction plan, and will continue to work closely with the Nuclear Regulatory Commission, Occupational Safety and Health Administration, and the National Institute for Occupational Safety and Health to minimize radiation exposure of workers and the public to levels as low as reasonably achievable. Additionally, DHS will continue to monitor environmental health and safety impacts associated with NII technology by constantly addressing these impacts with systems currently deployed and systems under development. As next-generation NII systems are developed, DNDO will make a constant effort to address environmental health and safety issues by consulting with the National Council on Radiation Protection and Measurements, and conducting modeling and benchmarking. This report was submitted in July 2007 and received no comments from Congress except for a request to make our findings open for distribution to the private sector. We complied with this request and modified the document so that it was no longer For Official Use Only (FOUO).

The two remaining reports, an overall investment strategy for radiological and nuclear detection across the U.S. Government, and a report on how DNDO authorization language impacted the Homeland Security Act of 2002 and DHS research and development efforts to detect, prevent, protect, and respond to chemical, biological, radiological, and nuclear terrorist attacks, are scheduled to be delivered in October. We are working with other DHS components and across the interagency to ensure

that these reports are comprehensive in nature and delivered to Congress in a timely manner.

The SAFE Port Act also required DNDO to establish an Intermodal Rail Radiation Detection Test Center. This was a very forward thinking requirement and one that DNDO strongly supports. There are several seaports that load cargo directly from ships to rail cars, therefore bypassing typical exit gate scanning operations. Right now, we do not have a detector that can address this challenge. An intermodal rail radiation detection test center will help develop additional passive detection design variants that meet unique port requirements, thereby enabling DNDO to provide solutions that enable us to scan 100 percent of cargo containers entering the United States. The test center was announced in May of this year and was awarded to the Port of Tacoma, Washington. The Port of Tacoma was chosen as the location of the Rail Test Center because more than 70 percent of its total import cargo volume is handled by rail at its multiple intermodal rail terminals. We are working diligently with the Port of Tacoma and CBP to begin testing the operational needs associated with intermodal rail, as well as evaluating innovative technical solutions to fit the unique radiological and nuclear detection requirements of intermodal terminals.

Additional Port Security Efforts

I wanted to take the opportunity today to also discuss additional port security efforts in which DNDO is involved. These are not outlined in the SAFE Port Act, but contribute to security in the maritime environment and for our country overall.

DNDO has an excellent working relationship with our Coast Guard operators. We have a joint acquisition plan in place that will allow DNDO to both develop and acquire systems for USCG use. DNDO provided handheld and backpack radiation detection devices to fulfill imminent operational needs in Fiscal Year 2007. We will deploy radiation detection capabilities to every Coast Guard inspection and boarding team by the end of 2007. The Secretary stated that this is one major goal for this Department, and we are going to meet that goal. We are also developing next-generation technologies that have the identification capabilities, connectivity, and ruggedness required in the maritime environment.

We also recently announced the West Coast Maritime pilot program that is beginning in the Puget Sound region of Washington State and will expand into San Diego, California. The three-year pilot will provide maritime radiation detection capabilities for State and local authorities with the goal of reducing the risk of radiological and nuclear threats that could be illicitly transported on recreational or small commercial vessels. We will be conducting this pilot program in close coordination with the U.S. Coast Guard and Customs and Border Protection. DNDO expects to deploy non-intrusive, passive detection sensors, such as human-portable radiation detection equipment, mobile sensors, and fixed-position detectors. We will also be working with maritime partners and local authorities in both areas to assess the geographic configurations of the ports to maximize detection and interdiction opportunities. Additional analyses for local partners will include a baseline survey of the existing radiological and nuclear detection architecture, a gap and risk assessment, and associated recommended actions to be developed in conjunction with maritime stakeholders. Maritime stakeholders will also receive guidance from DNDO on operational protocols, training, and exercises that support small vessel radiation detection capabilities.

Conclusion

The mission of the DNDO reaches far beyond port security. However, port security is a critical component in protecting the U.S. from nuclear terrorism. The SAFE Port Act codified many of the requirements and strategies that will ensure a robust defense against threats to our Nation. The DNDO and its partners have made significant progress over the last 2 years, and will continue to make progress in keeping this Nation safe. I look forward to working with all of our partners within DHS, other departments, State and local agencies, and the members of this subcommittee and Congress in continuing to pursue this goal.

This concludes my prepared statement. Chairman Inouye, Vice Chairman Stevens, and Members of the Committee, I thank you for this opportunity and request that this statement be submitted for the record.

PREPARED STATEMENT OF CHRISTOPHER KOCH, PRESIDENT AND CEO, WORLD SHIPPING COUNCIL

I. Introduction

The World Shipping Council is pleased to have the opportunity to submit the following comments to the Committee as it undertakes oversight of the various maritime programs and issues.

My name is Christopher Koch. I am President and CEO of the World Shipping Council (WSC or the Council), a trade association that represents the international liner shipping industry. I also serve as the Chairman of the National Maritime Security Advisory Committee (NMSAC), a Federal Advisory Committee Act committee providing advice to the Coast Guard and the Department of Homeland Security (DHS) on maritime security issues, and as a member of the Commercial Operations Advisory Committee (COAC) that advises the Departments of the Treasury and Homeland Security on commercial and Customs matters.

Liner shipping is the sector of the maritime shipping industry that offers service based on fixed schedules and itineraries. The World Shipping Council's liner shipping member companies provide an extensive network of services that connect American businesses and households to the rest of the world. WSC member lines carry roughly 95 percent of America's containerized international cargo.[1]

Approximately 1,000 ocean-going liner vessels, mostly containerships, make more than 22,000 U.S. port calls each year. More than 50,000 container loads of imports and exports are handled at U.S. ports each day, providing American importers and exporters with efficient transportation services to and from roughly 175 countries. Today, U.S. commerce is served by more than 125 weekly container services, an increase of over 60 percent since 1999.

In addition to containerships, liner shipping offers services operated by roll-on/roll-off or "ro-ro" vessels that are especially designed to handle a wide variety of vehicles, including everything from passenger cars to construction equipment. In 2006, these ro-ro ships brought almost four million passenger vehicles and light trucks valued at $83.6 billion into the U.S. and transported nearly one million of these units valued at $18 billion to U.S. trading partners in other countries.

Liner shipping is the heart of a global transportation system that connects American companies and consumers with the world. More than 70 percent of the $700 billion in U.S. ocean-borne commerce is transported via liner shipping companies.

The liner shipping industry has been determined by the Department of Homeland Security to be one of the elements of the Nation's "critical infrastructure".

Liner shipping generates more than one million American jobs and $38 billion in annual wages. This combined with other industry expenditures in the U.S. results in an industry contribution to U.S. GDP that exceeds $100 billion per year.

II. The Focus on Maritime Security

For the past 6 years, the WSC and its member companies have strongly supported the various efforts of the U.S. Coast Guard and U.S. Customs and Border Protection (CBP) to enhance maritime and cargo security. The multi-faceted and risk-based strategies and programs of the government have been able to make substantial progress toward meeting this challenge, and they continue to evolve. At the same time, the Coast Guard and CBP recognize the fact that the industry is transporting on average roughly 50,000 containers, holding roughly $1.3 billion worth of cargo owned by U.S. importers and exporters, each day through U.S. ports. Significant delays to this flow of legitimate commerce could have substantial adverse effects on the American economy.

The multi-layered maritime security strategy has a number of parts on which I will briefly comment today. The basic architecture of U.S. maritime security is well known and understandable. First, there is *vessel and port security,* overseen by the Coast Guard and guided in large measure by the International Ship and Port Facility Security Code (ISPS). Second, there is *personnel security,* overseen by various Department of Homeland Security agencies and the State Department. Third, is *cargo security,* which with regard to containerized cargo, is addressed through Customs and Border Protection's advance cargo screening initiative, C–TPAT, and the Container Security Initiative—all of which are reinforced and made more effective by the increased deployment of container inspection technology at U.S. and foreign ports.

---

[1] A listing of the Council's member companies and additional information about the Council can be found at *www.worldshipping.org.*

A. Vessel and Port Security Plans

Every commercial vessel arriving at a U.S. port and every port facility needs to have an approved security plan overseen by the Coast Guard. Each arriving vessel must provide the Coast Guard with an advance notice of arrival 96 hours prior to arriving at a U.S. port, including a list of all crew members aboard—each of whom must have a U.S. visa in order to get off the ship in a U.S. port.

The liner shipping industry's operations are consistent and repetitive—its vessel services and crews call at the same ports every week. So long as there is consistent and professional implementation of the security rules, which is usually a hallmark of the Coast Guard, liner shipping has found no problem in operating in the new vessel or port security environment.

We also appreciate the Coast Guard Commandant's admonition that the "concept of maritime security cannot be reduced to a single threat vector". There are numerous potential vectors for terrorists attack on the maritime environment that don't involve cargo containers. For example, merchant vessels are in fact defenseless against small boat attacks. We fully support the Coast Guard in its efforts to secure an enormous Maritime Domain against a variety of risks.

Long Range Information and Tracking (LRIT) of Vessels: On October 3, the Coast Guard published a Notice of Proposed Rulemaking (NPRM) on Long Range Information and Tracking (LRIT) in the *Federal Register*. The Council supports the LRIT objective and the enhanced visibility of vessels offshore that it will give to the Coast Guard and other governments.

The Coast Guard expects existing maritime satellite communications equipment to be able to meet these tracking requirements. Assuming this is correct, the Council does not foresee major problems complying with these regulations.

There may be concern, however, regarding how the Coast Guard intends to implement LRIT if the International Data Center (IDC) is not in place. The IDC is where a vessel whose country of registration has not established its own data center is to send its position reports. Many smaller nations were expected to use the IDC and how their vessels will comply with the LRIT requirements is in question. An agreement has been reached to allow the Coast Guard to host the International Data Exchange (IDE) on an interim basis until January 1, 2010. It is unclear what happens with the IDE after that date. A uniform, global operating system is the desired objective. The Coast Guard has invited comments on these issues in its recent NPRM, and we expect that the industry and other governments will be considering these issues closely.

Small Vessels: The attacks on the U.S.S. COLE and M/V LINDBERGH demonstrated that large vessels can be the objects of terrorist attack from small boats. The U.S. Coast Guard Commandant, Admiral Allen, has on numerous occasions noted this and other small boat vulnerabilities and the difficulty in devising effective ways to address the threat without significantly inconveniencing recreational and small boat movements. The Council notes that DHS has recently undertaken some pilot efforts on the West Coast to test technologies that may contribute to addressing this issue, and while we recognize the difficulty of the challenge, we believe that such DHS efforts are focusing on a legitimate concern. We also appreciate that the U.S. Coast Guard is playing a lead role in having put this on the International Maritime Organization's agenda in order to develop international principles and criteria for addressing this issue.

B. Transport Worker Identification Credential

The Council supports the credentialing of maritime workers requiring unescorted access to secure maritime facilities. The National Maritime Security Advisory Committee (NMSAC), with the advice and input of a wide range of U.S. maritime interests, has spent considerable effort to provide comments to the Coast Guard and the Transportation Security Administration on the development of the TWIC regime. The industry's primary concern is that the security enhancement envisioned in this new system not have undue impacts on those personnel who work in port terminals servicing vessels or on port operations.

The SAFE Port Act requires TWIC reader pilot projects to be run in at least five locations. NMSAC has recommended that the final TWIC regulations should not be published until the results of these pilot projects are known.

The Coast Guard has indicated its intention to issue two sets of proposed rules on the TWIC regulations: the initial set to give some shape to the pilots and the second, supplemental proposal which is intended to finalize the proposed regulations when the pilots' results are known. We support this measured approach.

The Coast Guard also recently announced the biometric standard to be placed on the TWIC card. This standard contains two items that were not supported by the industry: encryption and a Personal Identification Number (PIN). The industry's

concern has been that encryption will create operational complexities which have the potential to severely impede the flow of maritime commerce. Further, the NMSAC does not believe the significant additional costs associated with encrypting the fingerprint template are warranted given the minimal risk involved without such encryption. How these two items will work with readers remains to be seen, but the industry is hopeful that the good consultative process that the Coast Guard has established with NMSAC will allow for these issues to be addressed satisfactorily.

Lastly, DHS has begun to enroll workers in Wilmington, Delaware, starting on October 16, and has also listed the next eleven follow-on locations for enrollment. The industry strongly supports a measured implementation of this challenging new regime so that any unanticipated issues that may arise can be addressed as the system is rolled out in stages.

C. Containerized Cargo Security

The WSC fully supports the U.S. Government's strategy in addressing containerized cargo security. Specifically, the Council supports CBP's risk assessment and screening of 100 percent of all containers prior to their being loaded onto vessels destined for the U.S., and the pre-vessel loading inspection of 100 percent of those containers that CBP's cargo risk assessment system determines to present a significant security risk or question. The Council does not support recent legislation's call for inspection of 100 percent of all import containers before vessel loading, because the concept has not been clearly considered and remains presently impractical.

1. Container Security Initiative (CSI)

The network of bilateral Customs-to-Customs agreements forming the "Container Security Initiative" (CSI) continues to grow. There are now 58 foreign ports participating with the U.S. in this initiative, covering 85 percent of U.S. containerized import trade. CSI is a keystone to the effective international implementation of the advanced screening and inspection of U.S. containerized cargo that presents security questions. It is only through these cooperative CSI Customs-to-Customs data sharing and container inspection cooperative efforts that overseas container inspection can occur.

The Council recently wrote to CBP to recommend that the agency plan for how to expand its CSI Customs-to-Customs cooperative partnerships with European customs authorities to prepare for the planned 2009 implementation of the European 24 Hour Rule under Commission Regulation 1875. The purpose of such planning would be to ensure that American export containers receives the same kind of cooperative and expedited consideration when European authorities raise security questions, as European export containers receive today when CBP raises such a question.

2. Containerized Cargo Screening and Risk Assessment

CBP employs a multi-faceted containerized cargo risk assessment and screening system, so that it can identify those cargo shipments that warrant further review, rather than those that are low risk and should be allowed to be transported without delay.

C–TPAT: One element of that system is the Customs-Trade Partnership Against Terrorism (C–TPAT) pursuant to which various entities in the supply chain voluntarily undertake security enhancing measures. CBP then validates participants' compliance, and compliant supply chains are accordingly afforded lower risk assessments.

24-Hour Rule: Another important element of the risk assessment system is CBP's receipt and analysis of pertinent advance information about cargo shipments before vessel loading. This program began soon after September 11, under which carriers provide CBP with the advance shipment information they possess 24 hours before vessel loading in a foreign port for risk screening (the "24-Hour Rule"). The Council has fully supported this regulation and this strategy, which allows the CSI program to perform advance container risk assessment.

Better Security Screening Data: "10 plus 2" Initiative: While the 24 Hour Rule has been in the Council's view a logical and sound effort, the Council has for several years noted that more effective advance cargo security screening will require more data than the information provided by carriers via the 24 Hour Rule.

Recognizing both this need for enhanced container security targeting and the existing limits of information provided in carriers' bills of lading, the SAFE Port Act sets forth the following requirement to enhance the capability of CBP's Automated Targeting System:

> "Section 203(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 elements of entry data* . . . 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 ports.*"

Customs and Border Protection (CBP) is developing a regulatory proposal that would require U.S. importers or cargo owners to file ten additional data elements [2] with CBP 24 hours prior to vessel loading, and to require ocean carriers to provide two additional sources of data—vessel stowage plans prior to arrival in the U.S., as well copies of electronic container status messages. This is referred to as the "10 plus 2" initiative.

CBP has undertaken extensive, transparent, and open consultation with the trade and carrier community in developing this proposal. It is our understanding that the proposed regulation to implement this new requirement should be published in the *Federal Register* for public comment in the near future, with implementation beginning sometime in 2008.

While the private sector obviously needs to await the actual proposed regulation before providing comments in the expected rulemaking, we would note that CBP's efforts in developing this initiative have been transparent, professional and cooperative, and are in pursuit of a strategic objective that is not only mandated by the SAFE Port Act, but is highly logical in order to enhance containerized cargo risk screening.

Global Trade Exchange (GTX): Other pending efforts within DHS regarding the acquisition of additional cargo shipment information for enhanced risk screening are less understood by the trade. Notwithstanding the fact that CBP has not yet published, let alone implemented, its proposed "10 plus 2" regulations requiring additional information for cargo risk assessment, DHS officials have indicated that the Department will be proceeding with efforts to commence an additional trade data gathering and analysis effort under the name of the "Global Trade Exchange" or GTX.

This initiative has not yet been clearly explained to the industry, and there has not yet been any public transparency or opportunity to comment on the initiative.

What we understand at the present time is that DHS is considering awarding funding for an initial phase of this initiative. It is our understanding that participation by members of the trade providing such additional data is expected to be voluntary, that the party to collect the data would be drawn from a restricted number of commercial entities acting as a third party data clearinghouse, and that secure and confidential treatment of any data provided is recognized to be needed.

What services, analysis or risk assessment competence would be required of such vendors is unclear. What the specific data to be gathered would be has not been explained. The extent to which such shipment data would be shared with other governments is not clear. How this system would be integrated into CBP's existing Automated Targeting System is unclear. How such a commercial third party data manager would make money off this program is unclear, and who would bear what costs for participating in such a system is unclear. How the data in the system would be protected is unclear. Whether ocean carriers would be expected or invited to participate in the provision of information is unclear. What benefit would result from participating in such an effort is unclear.

DHS has indicated that the intent is to proceed under a "request for quotation" solicitation process, which is restricted to a limited number of vendors now established in the DHS "EAGLE" procurement program.

In short, the GTX effort has not yet been explained by the government and is not yet understood by the trade. U.S. importers with whom the Council has discussed this initiative are confused by this process. There is concern within the trade community over the apparent development of such an initiative without the government's usual transparency and process of consultation. That concern would likely be exacerbated if public review and comment were not requested, allowed or considered prior to the restricted procurement solicitation that is expected.

---

[2] The ten cargo data elements of the new Security Filing have been identified by CBP as: (1) Manufacturer (or Supplier) Name and Address, (2) Seller (or Owner) Name and Address, (3) Buyer (or Owner) Name and Address, (4) Ship To Name and Address, (5) Container Stuffing Location(s), (6) Consolidator (or Stuffer) Name and Address, (7) Importer of Record Number, (8) Consignee Number, (9) Country of Origin, and (10) Commodity 6-Digit HTS Code.

3. Container Inspection

DHS has a well established strategy to undertake radiation scanning of all containers entering the U.S. before they leave a U.S. port. CBP recently deployed its 1000th container radiation portal monitor as it gets closer to its objective of performing radiation scanning on 100 percent of all inbound containers at U.S. ports of discharge.

CBP also undertakes non-intrusive inspection technology (NII) or physical inspection of 100 percent of all arriving containers that are determined to pose a significant security question. CBP has no plans and no capability, however, to inspect every arriving container. Because that is not practical, the agency is utilizing, and soon will be enhancing, its cargo risk assessment system and the CSI program to identify which containers do warrant inspection.

In order to further consider the issues involved in the application of additional container inspection at *overseas* ports of loading, DHS has undertaken the "Secure Freight Initiative", under which pilot projects are being established at several foreign ports testing more complete pre-vessel loading scanning, generating possible lessons to be learned for broader application of pre-vessel loading container inspection efforts.[3]

The "Implementing the 9/11 Commission Recommendations Act", which was signed into law in August, includes the well known provision requiring that by 2012 100 percent of the containers imported into the United States be "scanned" before being loaded aboard vessels destined for the United States, meaning that the container would have be run through radiation detection equipment *and* non-intrusive imaging equipment before vessel loading. What, if anything, would be done with the images or data produced by those scannings was not addressed by the law, nor were a host of other highly relevant questions, including who was to perform this task, and whether the U.S. would perform such scanning of its own export containerized cargo. The WSC issued a six page statement on this legislation on July 30, which is attached to this testimony as Attachment A.

A number of other governments are obviously and justifiably concerned about the implications and meaning of this new U.S. law. We expect that they will continue to inform the U.S. Government of their concerns, including their view that this statutory provision expects foreign governments to undertake measures for their exports that the U.S. Government has no intention to undertake for its exports. The shipping industry's customers—the hundreds of thousands of U.S. importers and exporters who use containers to transport their cargo—are also concerned about the potential effects of this law.

Several things seem clear. First, implementation of this law's stated objective would require addressing many serious issues that the statute does not address, including the fact that implementation of overseas container inspection requires the cooperation of foreign governments. Second, the U.S. Government has no current plans to scan 100 percent of its outbound export cargo containers, and thus foreign governments' predictable inquiries about reciprocity will likely be unanswerable. And, if the United States' trading partners do not implement 100 percent container scanning, there is nothing that the U.S. Government can realistically do about it other than cease trading with the rest of the world. We therefore see the obvious need for further international dialogue on this matter.

4. Seals and Container Security Devices

The SAFE Port Act included the following directive: "Not later than 90 days after the date of enactment of this Act, the Secretary shall initiate a rulemaking proceeding to establish minimum standards and procedures for securing containers in transit to the United States." (Section 204(a)) It was not evident what this provision meant or how it might be interpreted, and the section's time deadlines were not going to be met.

Accordingly, the "9/11 Commission Recommendations Act", Congress amended this section by providing that: "(B) Interim Requirement.—If the interim final rule described . . . is not issued by April 1, 2008, then . . . 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. . . ." Thus by next October, all U.S. inbound containers will be required at a minimum to have ISO standard security *seals*.

---

[3] DHS has established three full scale container scanning pilots in co-operation with host governments at Southampton, U.K.; Puerto Cortes, Honduras and Port Qasim, Pakistan. Three other smaller scale pilots are under development at port facilities in Busan, South Korea (Gamman Terminal); Salalah, Oman, and Singapore.

As to the Government's view of "container security devices" (CSDs), things are less clear. The Council has understood that DHS was planning to issue proposed draft technical requirements for container security devices and the operating protocols associated with such devices by the end of this year for public review and comment. We understand that the DHS Science and Technology directorate prepared a draft of such requirements that is undergoing further review and amendment within the Department.

The Council and other members of the trade have requested that CBP/DHS allow for full transparency into the development of this effort and solicit public comments on the draft requirements, after they have completed internal government review.

There are at present many unanswered questions about CSD requirements, including what specifically the device would be required to do and its security value, what acceptable false positive and false negative reading rates would be, what radio frequency would be used, the requirements for the installation and operation of the necessary device reader infrastructure, the requirements applicable to the necessary communications interface and protocols with CBP, the security vulnerabilities of such devices, the necessity of interoperability of various vendors' devices and systems, the data to be captured and transmitted by the device, identification of who will have access to the data in the device, survivability and vulnerability of the device, power or battery life requirements, the probability that the device can be detected or removed without detection, required data messaging formats, event logs, and data encryption.

There has been little light or transparency provided on these issues, although in fairness, they are not simple issues. The Council believes it is essential, if an interest in CSDs is to be pursued, for the government to undertake a fully transparent and very clear articulation of its draft views on the requirements for such technology and the related operating systems and protocols, and to provide the public with a meaningful opportunity to comment upon such draft requirements, *before* they are advanced as an element of the government's container security strategy.

D. Port of New York's Recommendation for New Container Taxes

At the Committee's hearing on October 4, the witness for the Port Authority of New York and New Jersey expressed support for new "legislation establishing a uniform, nationwide Port Security User Fee to help offset growing port security costs."

This is a bad idea for many reasons.

First, it is relevant to note that the view of the Port of New York's witness at the hearing is not the position of the American Association of Port Authorities.

Second, when the Coast Guard promulgated its maritime security regulations in 2003 implementing the Maritime Transportation Security Act of 2002, it projected that the cost of compliance for the industry would be $7.331 billion over 10 years.[4] The New York Port Authority witness stated that the Federal Government has provided $1.3 billion in port security grants over the past 5 years, which is only a "fraction of the security costs that the industry has incurred over the same period" and that the regulations are an "unfunded mandate that industry has to bear".

The Coast Guard's cost estimates were of what the *industry* was going to have to spend to comply with its regulations, not the amount of money the government needed to provide the Nation's ports. Further, most of these expenses are already being incurred by the private sector carriers, terminal operators and cargo owners, without any Federal assistance.

Under the rationale of the Port of New York, it would appear that every regulation the government produces that has compliance costs is an "unfunded mandate". It seems a novel proposition indeed that the Federal Government should be responsible for all the costs that industry incurs in complying with government regulatory requirements. It is frankly illogical to argue that because the industry's regulatory compliance costs are X, and the government has provided grants in an amount which less than X, that we need a new Federal tax to make up the difference. We believe that the port industry should be appreciative for the grants that have been provided, particularly considering that there has never been a very precise delineation of what port security grants should be used for.

Shippers, forwarders, brokers, carriers and marine terminal operators have all incurred substantial costs to comply with applicable security regulations and programs. They have not asked the government to pay for those compliance costs, What they do want is for the requirements to be well designed to improve security in a cost-effective manner.

---

[4] First year estimated cost of implementation was approximately $1.5 billion, with an annual cost of approximately $884 million. Implementation of National Maritime Security Initiatives, 68 Fed.Reg. 60448, 60464 (Oct. 22, 2003).

Third, the Port of New York witness did not identify with any specificity what such Federal port security grant money is needed for, or why it is the responsibility of all cargo containers across the Nation to provide it. We appreciate that the Port of New York witness notes that entities in the Port of New York and New Jersey have received 12 percent of total port security grant funding and that the Port apparently believes that it should receive a higher share; however, as explained below, there is an existing mechanism for the port to increase its revenue collection to cover higher costs if it is important to do so.

Fourth, and perhaps most importantly, ports currently have and use the authority and capability to collect additional funds they need for security at their facilities from their commercial customers. Today, as the Port of New York witness noted, ports throughout the U.S. and abroad are assessing and collecting port security charges from their commercial customers. They also have antitrust immunity under the Shipping Act to collectively establish such charges if the wish to do so. There is no need for a new Federal tax. Though questions of equity and appropriateness of such fees obviously should be addressed on a case-by-case basis, the very fact that the ports' customers, including the members of the World Shipping Council, are presently paying these port security fees belies the notion that extensive new Federal taxes or "user fees" are warranted.

Finally, the Port of New York witness noted concern that U.S. seaports should not be put at a "serious disadvantage in relation to ports in Canada and Mexico." We question whether ports such as Seattle and Tacoma would see a new national tax on commerce going through their ports to pay for more grants to the Port of New York as doing anything other than disadvantaging them in relation to ports in Canada.

III. Conclusion

Vigilance against terrorist risks requires the development and implementation of prudent security measures, and the continuing enhancement of such measures as the risks change and take new forms. The international trading system is too valuable and important to be left unattended.

The liner shipping industry fully understands this and has cooperated with national governments and international organizations trying to construct meaningful security regimes. The industry will always be concerned that these measures not unduly delay or restrict commerce or impose costs that produce little added security; however, it has supported and will continue to support measures that are well designed and provide real security value with as little impact as possible on legitimate trade.

This is clearly difficult work, but there are clearly some success stories. The International Maritime Organization's development of the International Ship and Port Facility Security (ISPS) Code, the Proliferation Security Initiative, the Container Security Initiative, the "24 Hour Rule" advance cargo screening strategy and its imminent enhancement, the C–TPAT program—all have enhanced supply chain and maritime security. The government's expanded use of container inspection technologies is another example of sound strategy and implementation.

If we are to continue to make progress in enhancing maritime and supply chain security, progress is more likely to occur if:

1. There is a clear and specific definition and agreement on what should be done to improve security.
2. There is a clear and thoughtful prioritization of initiatives.
3. There is sufficient certainty and clarity in purpose to do it right. In the absence of that, time and resources are poorly used and the efforts are less likely to improve security.

We appreciate the Committee's continued interest and oversight of these issues, and would be pleased to provide additional information that may be of assistance to the government in addressing these issues.

ATTACHMENT A

WORLD SHIPPING COUNCIL—STATEMENT REGARDING LEGISLATION TO REQUIRE 100% CONTAINER SCANNING—July 30, 2007

The first session of the 110th Congress has enacted H.R. 1, the "9/11 Commission Recommendations" legislation, which the President has said he will sign. Included in that legislation is a provision, which was *not* a recommendation of the 9/11 Commission, that requires, effective July 2012, that all maritime cargo containers being

imported into the United States must be "scanned" at foreign ports of loading or they will be denied entry into the country.

This so-called "100 percent scanning", or "100 percent container inspection" requirement as it is sometimes called, was opposed by the Department of Homeland Security (DHS), Customs and Border Protection, present and former government security experts, the U.S. Chamber of Commerce, all major cargo shipper organizations, the ocean carriers transporting the cargo, as well as the European Commission and the governments of America's trading partners, including Belgium, Canada, Denmark, Finland, France, Germany, Greece, Italy, Japan, the Netherlands, Norway, Poland, Portugal, Singapore, Spain, Sweden, and the United Kingdom.

Why was such a proposal opposed by virtually all elements of the global trading system? Was it because of cost? No. Was it because of a lack of commitment to enhancing cargo security? No. It was in the words of the *Washington Post* "a bad idea" and "a slogan not a solution". It was because the legislation is not only unworkable, but that the Congress failed to even try to address fundamentally critical questions about how such a system would actually operate.

The New Law

The legislation provides:

> "(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)."

The Problems

The House passed H.R. 1 without having Committee hearings or allowing floor amendments on this issue. The Senate did not have a hearing on these issues.

Nevertheless, every one of the following issues was repeatedly brought to the attention of the Congress by numerous parties, but without effect.

1. *Pilot Programs Ignored:* Pursuant to the SAFE Port Act passed by the Congress just last year, the Department of Homeland Security has established pilot programs under the "Secure Freight Initiative" in a number of ports around the world to test the concept of scanning containers loaded onto ships destined for the U.S. Those pilots are still underway, and their lessons have not been examined or considered.

2. *Failure to Define Who is To Perform the Container Scanning:* It would seem elementary that U.S. legislation requiring every container to be scanned before being loaded onto a vessel in a foreign port would address the issue of who is to perform this activity. This legislation fails to do so. It does not require U.S. Customs to do this, as it is clearly impossible for the Congress to require U.S. Customs to undertake such activities within the jurisdiction of other sovereign nations. It does not require foreign governments to do so, as it has no such authority. The legislation simply says that containers shall be scanned. By whom? By governments? By foreign port facility operators? The Members of Congress sponsoring this legislation took the position only last Congress that one of the largest port facility operators in the world, Dubai Ports World, was an unacceptable security risk to buy a U.S. marine terminal operating company and hire U.S. workers to service vessels in U.S. ports. Is that company, and other private terminal operating companies, now who Congress looks to scan U.S.-bound containers in foreign ports? Does Congress care who performs this activity? If Dubai Ports World now undertook this role, would the Congress approve such a role? One would think such a basic question would have been subject to some examination by the Congress and some answers.

3. *Failure to Define Who is to Purchase, Operate and Maintain the Technology:* Related to the above question, is the failure of the legislation to define who is expected to undertake the substantial capital commitments and operational responsibilities to implement such a system.

4. *Failure to Address Health and Safety Issues:* The legislation fails to recognize the need to address the health and safety issues relating to the use of this equipment. Even if the equipment performs to the U.S. Government's health and safety regulatory requirements, other governments have different standards. Furthermore, labor and workforce acceptance of driving through non-intrusive imaging (NII) equipment remains a significant issue. U.S. port labor will not do so. As a practical

matter, this legislation requires the rest of the world to do what cannot be done today in U.S. ports.

5. *Failure to Seek or Obtain the Necessary Cooperation of Other Governments:* No expansion of overseas container inspection will occur without the cooperation and consent of foreign governments. This law fails to even acknowledge the need for their cooperation. Customs and Border Protection has spent considerable effort since 9/11 to build cooperative bilateral Customs-to-Customs working agreements at seaports around the world through its Container Security Initiative (CSI). The success of CSI is based on mutual respect, recognition of other nations' sovereignty, cost sharing, and targeted priorities. This legislative mandate is devoid of those qualities.

6. *Failure to "Practice What You Preach"—No Reciprocity:* Congress was repeatedly advised of the difficulty of this legislation's requiring 600 ports around the world to approve, implement and utilize such technology, systems and processes for all cargo destined for the U.S. or effectively face an embargo on their exports, when the U.S. Government does not even try to perform this function on its export cargo, scans virtually zero U.S. export containers, and has no plans to do so. If implementation of this law is actually pursued, it is entirely possible, if not highly likely, that foreign governments would establish "mirror image" requirements on the U.S., forcing all American export containers to undergo radiation and NII scanning before vessel loading at U.S. ports—requirements which the U.S. Government and U.S. port facility operators are presently and for the foreseeable future incapable of meeting.

7. *Failure to Define the Scanning Requirement:* Congress recognized that 100 percent container "inspection" is impractical and therefore requires instead that every container be "scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign port before it was loaded on a vessel." This by itself would be pointless. The law fails to address what is to be done with the scanning data generated, whether or when the data from the scanning equipment is transmitted to the U.S. Government, or who is to analyze the data generated.

8. *Failure to Address Scanning Analysis Responsibility:* The law fails to address whether the scanning data actually has to be reviewed and analyzed, and if so, under what circumstance, when and by whom? In essence, it fails to identify how the technology is to be used. Will the images of every scanned container have to be reviewed? If not, when are the images to be reviewed and by whom? Are they simply to be filed in an electronic library somewhere? If so, is it reasonable to ask other nations to invest hundreds of millions of dollars in such equipment, plus labor, maintenance and operating costs, if these images will only be used on an exception basis or for "forensics"? This cost/benefit question is even more relevant in light of Members of Congress' criticisms of the efficacy of the equipment currently being used for these purposes by DHS, especially after questions about such equipment were recently raised by the Government Accountability Office. Further, the law fails to try to address what is done if one of the scans identifies an anomaly that requires secondary inspection—a common occurrence with the use of these technologies. These are fundamentally important issues with difficult operating protocols and significant costs associated with them—all of which the legislation does not address.

"Extension" Authority

Recognizing that this legislation has fundamental problems, some have noted that the law grants the Department of Homeland Security discretion to extend the effective date of the requirement. Before examining that part of the legislation, it is important to note that the law does not allow DHS to amend or adjust the law's requirement, only to extend the effective date of the 100 percent container scanning requirement.

The law provides:

> "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."

It is presumably the ambiguity and flexibility of this language that has allowed the President to sign this legislation, as it might be used to extend these requirements, perhaps indefinitely, although that is not clear and could be arguable.

Criteria (A) would seem meaningless as a justification for extension, as radiation and NII scanning systems are "available". Criteria (C) is of limited application because ports' "physical characteristics" are not generally among the principal issues involved with implementing such a concept. Criteria (D) does not define what "existing systems" means. Criteria (B) and (F) are confusing because NII scanning equipment, unlike radiation scanning equipment, neither produces "alarms" nor "automatic notification of questionable or higher risk cargo". So what does this mean?

Without belaboring the point, the "extension" authority portion of the legislation is unclear, but the Administration would seem to have some ability to avoid application of the implementation date of the law.

It is therefore odd, disconcerting, yet entirely predictable that this legislation produces both statements from Members of Congress that the law will require 100 percent container scanning at foreign ports by 2012, and statements from other observers that the law is wholly impractical and thus it is unlikely to be applied because the U.S. Government will not cut off its own commerce with countries that do not implement 100 percent container scanning before vessel loading.

This provides little comfort or certainty to governments and ports around the world that are trying to understand what this legislation passed by the Congress of the United States actually means and what its implications are.

The Path Forward

Roughly $500 billion of annual American commerce is affected by this law.

What is clear is that this issue deserved a more open process of analysis and debate, that other governments resent the unilateral dictates and hypocrisy in the law, and that there are over 600 ports around the world trying to figure out what this legislation means.

The issue of how to continuously improve containerized cargo security is important to the American public, to American commerce, and to the shippers and carriers and ports involved.

There are a range of existing efforts to address this challenge, including:

- the "24-Hour Rule" and the advance screening and risk assessment of cargo shipment information before vessel loading for 100 percent of all containers coming to the U.S.;
- the Container Security Initiative noted earlier;
- the Customs-Trade Partnership Against Terrorism initiative;
- the radiation screening of virtually every container arriving at a U.S. port;
- the inspection of every container that Customs and Border Protection believes presents a significant security question;
- security plans overseen by the Coast Guard for every vessel entering a U.S. port and every port facility;
- the Department of Energy's "Megaports Initiative", which provides radiation detection equipment and trains personnel abroad to check for nuclear materials. In exchange, DOE requires that data be shared on detections and seizures that resulted from the use of the equipment. This initiative and the CSI initiative are collaborative efforts by two different U.S. agencies, DOE and DHS, working with host countries to reduce the risk of terrorism;
- the International Port and Security Program (IPSP) initiative, under which the U.S. Coast Guard and host countries work together to evaluate compliance with the International Ship and Port Facility Security (ISPS) Code. This information improves U.S. and foreign security practices, and helps assess if additional security precautions will be required for vessels arriving in the U.S. from other countries;

- as well as two major emerging DHS initiatives—the "10 plus 2" program, under which Customs and Border Protection will require importers to provide 10 additional data elements before vessel loading for enhanced security targeting and 2 additional streams of operating data from ocean carriers to assist in the tracking of container movements, and the Transportation Worker Identification Credential that will provide DHS security screening of transportation workers.

Neither the government nor the industry is ignoring the enhancement of maritime security.

To the extent a vision for 100 percent container scanning of containers on a global basis is to be moved forward, it will require a more open, consultative examination of the real world issues involved than what transpired in the debate and enactment of H.R. 1.

PANJIVA
New York, NY, October 3, 2007

Senate Committee on Commerce, Science, and Transportation,
Washington, DC.

To Whom It May Concern:

Panjiva gives businesses the tools to secure their supply chains. We do this by helping companies find reliable overseas suppliers. Given our expertise we are writing to recommend actions that we believe will secure our ports by securing America's supply chain.

We welcome this opportunity to submit testimony to the Committee on Commerce, Science, and Transportation. Fundamentally, we have two recommendations to secure our ports, not only from terrorism but also from tainted imports. They are (1) focus on the supplier, and (2) promote existing private sector resources. For each recommendation, we outline our rationale and then offer an explanation of the actions that we would like to see taken.

Panjiva was founded on the principle that information is a powerful tool to direct global trade. We have spent the last few years developing technology to clean, integrate and analyze data from various sources to evaluate overseas suppliers. We could not have foreseen the coming storm of high-profile recalls and the heightened concern about import safety. However, we were not surprised either. With an ever-increasing volume of imports and very little quality information available, America's supply chain was susceptible. Panjiva exists because we saw the need for a revolutionary, objective data source to inform global trade.

The challenges of improving import safety and port security can only be met by the government and private sector working together. We wish to thank the Members of the Senate Commerce Committee for their initiative on this important issue. If Panjiva can be helpful in any way, please do not hesitate to contact us.

Thank you for your consideration.

Sincerely,

JOSH GREEN
Chief Executive Officer
JAMES PSOTA
Chief Technology Officer

Recommendation #1: Focus on the Supplier

Overview:

- Government agencies should maintain a database of profiles for all suppliers to U.S. markets
- Each supplier should be assigned a unique PIN# to link customs data to supplier profiles
- Each supplier should be assessed as high, medium or low risk based on its track record

Rationale:

- The inability to inspect our way to safety necessitates a risk-based approach.
- An ever-increasing volume of imports requires targeting inspections at high-risk shipments.
- There is a limitation to current thinking that only assesses risk by looking at the imported product itself or its country of origin:

- *Country of Origin:* Despite a recent focus on China, it is impossible and undesirable to inspect all Chinese imports, the vast majority of which are from reliable sources.
- *The Life-Cycle of the Import:* Although awareness of "risks over the life cycle of an imported product" is an improvement over simply screening imports at the border, tracking particular imports still provides an incomplete picture.

- The International Trade Data System (ITDS) is a valuable tool but government agencies must seek new data sources to enable the targeting of resources to areas of greatest risk.
- A supplier's track record is an indicator of risk associated with shipments from that supplier.
- A database of supplier profiles to supplement the ITDS will allow government agencies to assess the risk of shipments based on the prior track record of the supplier and in doing so encourage suppliers to build a track record of reliability.
- Panjiva's success in providing objective information to the private sector about overseas suppliers demonstrates that this is an attainable goal for government as well.

Explanation of the Recommendation:

Government agencies need the means to assess the risk associated with suppliers of imported products because some suppliers are riskier than others. All else being equal, suppliers that have served U.S. markets for years without incident are less risky than suppliers that are serving U.S. markets for the first time. All else being equal, suppliers that have been independently certified as living up to international standards of public safety are less risky than suppliers that have never been certified. Suppliers should be encouraged to build a track record of reliability, and heightened attention should be paid to shipments from suppliers that have been unreliable in the past.

A database of supplier profiles is an important tool to enable the targeting of resources to areas of greatest risk. Every profile would record the supplier's history of importing goods into the United States. Based on their track record, each supplier will be assessed as high risk, medium risk or low risk. Government agencies can focus their limited resources on shipments that are coming from suppliers that have been deemed high risk. Each supplier should also be assigned a numerical identifier or PIN# to facilitate linking customs data to supplier profiles. As Customs and Border Protection tracks imports entering the United States, they will be able to quickly identify the supplier and determine whether the supplier's history warrants increased scrutiny.

Recommendation #2: Promote Existing Private Sector Resources

Overview:

- Government should promote existing resources within the private sector that help companies adhere to high standards of reliability and secure their own supply chains.
- Government should seek to continually foster awareness of private sector resources and to reward companies that use private sector means to secure their supply chains.

Rationale:

- The challenges of improving import safety can only be met with a culture of collaboration between the government and the private sector.
- Just as important as developing new resources is the need to utilize existing resources.
- There is presently significant innovation in the private sector that aims to ensure adherence to high standards of reliability and to enable self-monitoring of the supply chain.
- Private sector efforts are as varied as certification agencies with over a century and a half of experience to revolutionary technologies that use data to inform trade decisions.
- Companies are not aware of all of the private sector options available and are not always attentive to the benefits that are associated with these options.
- A very small minority of overseas companies have sought any third-party certifications.

- The Federal Government has the opportunity to promote awareness of private sector options to every company that imports goods into the United States.
- If companies are aware of available options and are publicly recognized for self-monitoring efforts, they are more likely to take transparent steps to secure their own supply chains.

Explanation of the Recommendation:

The private sector already provides various means for companies to ensure adherence to high standards of reliability and to self-monitor their supply chains. Government must continually promote private sector innovation that helps companies achieve the goal of securing their supply chains. Private sector options should be publicized to companies already serving U.S. markets and made available to new companies seeking to import into the United States.

Resources made available to companies in the private sector include certification agencies, vendor compliance software, and information databases. SGS Group and Bureau Veritas have each provided more than a century of certification and inspection services to ensure a company's processes are compliant with standards of quality, health, safety, environment, as well as social responsibility. Underwriters Laboratories (UL) and Intertek conduct product testing and are trusted sources of product compliance certifications. Vendormate's technology allows for monitoring of vendor credentials and compliance. Panjiva provides an objective source of information to help companies find reliable overseas suppliers.

The Federal Government can support private sector innovation not only by promoting awareness of existing resources, but also by recognizing companies for their self-monitoring efforts. Currently, the Department of Homeland Security acknowledges and rewards companies with high standards of supply chain monitoring through the Customs-Trade Partnership Against Terrorism (C–TPAT). However, companies should be rewarded not only for prohibiting terrorist threats, but also for preventing the importation of tainted goods.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO REAR ADMIRAL DAVID P. PEKOSKE

Question 1. The GAO believes you will have difficulty meeting the domestic and international inspection requirements. Do you agree with GAO's assessment? Is the Coast Guard sufficiently staffed to conduct the domestic and foreign port inspections required under the SAFE Port Act? How many inspectors do you have trained and tasked to perform this requirement?

Answer. The Coast Guard is sufficiently staffed to conduct both foreign and domestic port inspections required by the SAFE Port Act. The Coast Guard received $15 million in FY 2007 specifically to support, among other initiatives, additional domestic and international inspection activities. This additional funding allowed the Coast Guard to hire additional personnel to meet the new SAFE Port Act requirements.

The domestic inspection program has 389 inspectors assigned and trained to conduct Maritime Transportation Security Act (MTSA) inspections at approximately 3,200 regulated facilities. As of 22 November 2007, the Coast Guard has conducted 8,100 inspections and spot checks of these facilities, which exceeds the requirements of the SAFE Port Act.

The international inspection program has 60 personnel assigned to coordinate, conduct and manage the foreign port inspections. The training process is dynamic and the number of trained assessment personnel fluctuates. However, there are sufficient trained personnel to conduct the program, and the Coast Guard is meeting associated SAFE Port Act requirements.

Question 2. In multiple reports and in testimony today, the GAO recently cites that the Coast Guard had a fundamental lack of resources to successfully perform its security missions on a wide range of activities including vessel escorts, harbor patrols, vessel boardings, domestic and international inspections, and the development of Interagency Operation Command Centers. Do you agree with their assessment?

Answer. Regarding domestic and international inspections, additional funds received in the Coast Guard's 2007 appropriation allowed the Coast Guard to hire additional staff in these areas, and the Coast Guard is meeting or exceeding the requirements of Sections 103 and 234 of the SAFE Port Act.

Regarding the development of Interagency Operation Command Centers, the Coast Guard submitted a cost-sharing analysis as required by Section 108 of the

SAFE Port Act which estimated the Coast Guard will need $260M over 5 years to meet the requirements of that section of the Act.

Regarding general security activities (escorts, patrols and boardings), the Coast Guard's guidance to field commanders, Operation *Neptune Shield,* prioritizes these activities based on risk and the availability of resources. Higher risk, higher consequence activities are provided with more attention and consideration than lower risk and consequence activities.

Question 3. What has the Coast Guard done to develop and implement the port security training and exercise programs required in the SAFE Port Act? How many workers do you expect will receive training in the next calendar year? What barriers, if any, do you foresee in implementing the training mandate?

Answer. The Coast Guard is meeting the requirements of Section 114 of the Act through its Area Maritime Security exercise program, which was implemented in October 2005 and funded with $10M from the Coast Guard's FY06 appropriation. This program exercises the Area Maritime Security Plan and/or Committee annually in accordance with 33 CFR Subchapter H. Over 45 exercises are conducted each year. The training is specific to the National Incident Management System. While the exercise program does not involve training of security workers, the Coast Guard and DHS are working with DOT on development of related courses. DOT can provide additional information if interested.

DHS has the lead on developing a program to meet Section 113 of the SAFE Port Act (Port Security Training Program). FEMA's National Preparedness Directorate's National Integration Center is developing a security training program for port facilities to fulfill SAFE Port Act requirements.

In addition, the Coast Guard has worked with MARAD to develop model courses for facility personnel to meet the requirements in Section 109 of the Maritime Transportation Security Act. These courses are currently being revised to include both SAFE Port Act and TWIC requirements.

We are also currently revising the regulations for security training for facility personnel to ensure all training is measured against a standard of competence, including the topics required under the SAFE Port Act.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO REAR ADMIRAL DAVID P. PEKOSKE

Question 1. Since 9/11, the Coast Guard has rapidly expanded the level of resources dedicated toward port security. According to a 2004 GAO report, the Coast Guard dedicated an average of 19,000 resource hours per year to port, waterway, and coastal security before 9/11. By 2003, the number of hours increased by over one thousand percent to over a quarter-million resource hours. What challenges and growing pains has the Coast Guard experienced during this massive shift in emphasis to port security?

Answer. Following the events of September 11th, the Coast Guard faced the challenge of rapidly expanding its role to include new activities designed to further safeguard national maritime interests from terrorist threats. The Coast Guard's approach addressing this challenge is comprised of maritime regimes, domain awareness and operational capabilities.

The broad challenge included a need to expand regulatory authorities to require better security measures from maritime stakeholders. The Coast Guard reviewed existing maritime regimes to identify gaps in our Nation's maritime security requirements. The service worked aggressively to lead the development of new international standards (the International Ship and Port Facility Security (ISPS) Code) and national regulations (Maritime Transportation Security Act of 2002) that apply to both foreign and U.S. flag commercial vessels entering our Nation's waters, as well as the port facilities used by those vessels.

Another part of the broad challenge after September 11th was the need to develop a better understanding and awareness of the maritime domain. The Coast Guard also led the way in identifying our Nation's broad information needs for maritime situational awareness which involved expanding Command, Control, Communications, Computers, Intelligence and Surveillance, and Reconnaissance (C4ISR) capabilities to provide a "picture" of conditions and activities across the maritime domain. Additionally, the current state of domain awareness has involved developing new and refining existing methods to collect, fuse, analyze and disseminate information to a wide range of users. Unprecedented levels of information sharing and intelligence integration have taken root and continue to be improved.

Finally, another major part of the challenge was for the Coast Guard to expand its own capabilities to address the new security paradigm. The Coast Guard worked

quickly to stand up new operational capabilities such as the Maritime Safety and Security Teams (MSSTs), develop protocols and procedures to protect our Nation's maritime infrastructure from terrorist threats and respond to terrorist incidents, and train CG boarding teams, vessel inspectors, and facility inspectors to conduct specialized security operations. Each of these efforts involved careful planning and integration of lessons-learned. As with all new activities, our processes and protocols are maturing with continued implementation and will inform future efforts as we strive to continually improve.

Question 2. Admiral Pekoske, as you know, the SAFE Port Act required the Coast Guard to establish Interagency Operations Command Centers at all high priority ports within 3 years from the date of enactment. The idea is if Federal, state, and local agencies with a role in port security are co-located, there will be greater sharing of intelligence and overall improved coordination. Seattle is now home to one of these Centers. Was the construction of these Centers completely dependent on Coast Guard funds? Where do the operational funds come from? How are the Centers staffed? Will they be dependent on individuals borrowed from other Federal agencies?

Answer. In an effort to fulfill Section 108 of the SAFE Port Act, which requires the Secretary to establish Interagency Operations Centers (IOC), the Coast Guard is planning increased coordination capabilities at all 35 Sector Command Centers and facility expansions at many. The actual degree of expansion and capability increase is yet to be determined, but will be coordinated with other Department initiatives such as SBINet and the USN's MDA Program.

Construction of the Seattle IOC was included in the rebuilding of the entire Sector complex, which was funded through Coast Guard appropriations. The Coast Guard funds the operation and maintenance of the Seattle facility. The U.S. Navy contributed to the center's sensor network and tracking systems. The Coast Guard and Navy have cost-sharing arrangements in place for the equipment maintenance.

The Seattle IOC is staffed by Coast Guard Sector Seattle Command Center personnel and representatives from approximately 16 Federal, State and local agencies. Some agencies provide full-time personnel, and other agencies may only provide one or two people as needed. The level and variety of Federal, State and local participation at IOCs will vary depending on the unique characteristics of the port. As in Sector Seattle, it is anticipated that participating agencies will provide personnel at agency expense.

Question 3. We all recognize that programs requiring participation from multiple Federal agencies and multiple levels of government present unique challenges with respect to the issue of mixing funds. Does the construction of these Centers face any jurisdictional or fiscal hurdles due to their interagency nature?

Answer. The Coast Guard is examining the legal authority to construct facilities that directly support personnel from other government agencies. Coast Guard's legal authority does not extend to funding for salaries for personnel working for other departments, agencies or organizations. Therefore, participating Federal, State and local agencies will have to commit financial and/or human resources to staff the Interagency Operations Centers.

Question 4. According to the Bush Administration's National Strategy for Maritime Security, "The maritime domain is the likely venue by which a weapon of mass destruction will be brought into the United States." If a terrorist group attempted to smuggle such a weapon into the U.S. using a container ship today, how confident are you that you will be able to detect and intercept the different types of WMDs?

Answer. The stated policy of the Coast Guard Maritime Radiation Detection Program is to detect and intercept radiological threats as far from U.S. ports as possible. The operational goal is to use Coast Guard boardings and inspections as a means to detect and intercept illicit radioactive material before it enters the United States.

If there is actionable intelligence concerning illicit radioactive material, the detection confidence level is relatively high. Such intelligence would be a trigger for initiating/activating the "Critical Incident Communications Network" and Maritime Operational Threat Response (MOTR) Plan Protocols, wherein appropriate intra-/interagency resources would be brought to bear to resolve the situation.

In boarding cases where no actionable intelligence is involved (the majority of boardings), all Coast Guard boarding teams are outfitted with and required to carry personal radiation detectors (PRDs). If radiation is detected, these boarding teams are trained to locate and determine if the source is legitimate. If they are unable to do so, a specialized Coast Guard team (equipped with wide-area radiation search devices and hand-held gamma spectrometers) would be called-in to locate the source and identify the radioisotope. The specialized team has the capability to "reach

back" and transmit their data to the DHS CBP Laboratory Scientific Services Teleforensics Center for further analysis and verification. If the radioactive source is determined to be illicit in nature, existing interagency agreements and initiation of MOTR Plan protocols would be used to bring in the necessary resources (*e.g.,* Department of Energy, Federal Bureau of Investigations, etc.) to resolve the situation.

A limiting factor in determining the detection confidence level is whether or not the radiological material is shielded or unshielded. With currently fielded, state-of-the-art equipment, a shielded source is much more difficult to detect. As a result, the Coast Guard is working very closely with the Department's Domestic Nuclear Detection Office (DNDO) in the development of next-generation detection/identification equipment (suited to the maritime environment) to increase detection and identification of shielded sources.

Chemical and biological agents are very difficult to detect when properly contained. Presently, the Coast Guard boarding crews use a four-gas monitor that will test for acceptable Oxygen (O_2) levels, presence of Hydrogen Sulfide (H_2S), Carbon Monoxide (CO), and combustible atmospheres Lower Explosive Limits (LEL). Additionally, crews have the "HazMat Smart Strip" that changes color when exposed to dangerous chemicals. A change in color in any of eight categories alerts personnel to the potential presence of chemical agents. If there is actionable intelligence about a potential/actual smuggled agent, the Coast Guard would deploy the Maritime Security Response Team (MSRT) or National Strike Force (NSF), which have advanced Chemical Warfare Agent (CWA) and Toxic Industrial Chemical (TIC) detection capabilities. The Coast Guard does not use biological detection devices during boardings at this time. We recommend CBP add their screenings and targeting efforts to this DHS response.

In addition, Customs and Border Protection (CBP) implements a layered approach to container security, utilizing of a number of different programs designed to detect and interdict weapons of mass destruction or weapons of mass effect.

These programs include the Container Security Initiative (CSI), the Automated Targeting System (ATS), the Customs-Trade Partnership Against Terrorism program (C–TPAT), and the Non-Intrusive Inspection (NII) program.

CSI is the only multinational program in the world actually protecting the primary system of global trade—containerized shipping—from being exploited or disrupted by international terrorists. Its core elements are: identifying high-risk containers-through the use of automated targeting tools to identify containers that pose a potential risk of terrorism, based on advance shipping information and strategic intelligence; screening and evaluating containers before they are shipped—containers are screened as early in the supply chain as possible, generally at the last port of lading; and the use of technology to scan high-risk containers to ensure that scanning can be done rapidly without impeding the movement of trade—this technology includes large-scale X-ray, gamma ray machines and/or radiation detection devices.

The C–TPAT program is CBP's premier trade security program. C–TPAT partners CBP with the trade community for the purpose of securing the U.S. and international supply chains from possible intrusion by terrorist organizations. C–TPAT requires the trade community participant to document and validate their supply chain security procedures in relation to existing CBP C–TPAT criteria or guidelines as applicable. CBP requires that C–TPAT company participants develop an internal validation process to ensure the existence of security measures documented in their Supply Chain Security Profile and in any supplemental information provided to CBP. As a part of the C–TPAT process, CBP C–TPAT Supply Chain Security Specialists and the C–TPAT participants will jointly conduct a validation of the company's supply chain security procedures. The validation process is essential to verifying the company's commitment to C–TPAT.

As trade increases, CBP's reliance on NII technology, the cornerstone of CBP's multi-layered strategy to secure the borders, becomes more and more critical. Since an adversary can defeat any single sensor or device, CBP does not rely on any single technology or inspection process. Instead, CBP uses various technologies in different combinations to substantially increase the likelihood that a nuclear or radiological weapon or weapons grade material will be detected. Technologies deployed to our Nation's land, sea, and airports of entry include large-scale X-ray and gamma-ray imaging systems, as well as a variety of portable and handheld technologies, and radiation detection technology.

At the core of CBP's ability to achieve its critical border security objectives and maintain the flow of lawful commerce is the ability to identify high-risk travelers and goods for inspection while allowing the vast majority of law-abiding travelers and commerce to move without unnecessary delay. Recent legislation and regulatory action, such as the Trade Act of 2002, the 24-hour rule, and the SAFE Port Act,

have made it mandatory to provide advance information about passengers and goods arriving in the United States. CBP uses computer technology and rule-based software to analyze the data provided on passengers and shipments arriving in the United States. CBP applies its targeting methods against the data to determine which passengers or shipments need to be segregated for a closer look and possible intensive inspection.

The main platform used to perform this analysis is the Automated Targeting System (ATS). The ATS and associated databases provide CBP Officers (including those stationed overseas at Container Security Initiative ports) with advanced notice of travelers and goods arriving at U.S. ports of entry, allowing them to cross-check the passenger and cargo manifests against databases such as the Traveler Enforcement Compliance System (TECS), the Interagency Border Inspection System (IBIS), and National Crime Information Center (NCIC) for "lookouts" for unlawful activity. CBP also uses ATS to analyze data in the Automated Export System (AES) on shipments leaving the U.S.

CBP recently implemented an added security layer with the Secure Freight Initiative (SFI). On December 7, 2006, the Department of Homeland Security (DHS) and the Department of Energy (DOE), in cooperation with the maritime industry and foreign government partners, announced Phase I of SFI.

The SFI program is an unprecedented effort to build upon existing port security measures, like CSI and DOE's Megaports Initiative (MI), by enhancing the United States Government's ability to scan containers for nuclear and radiological materials in seaports worldwide and to better assess the risk of inbound containers.

The initial phase of the Secure Freight Initiative involves the deployment of a combination of existing technology and proven nuclear detection devices to seven foreign ports: Port Qasim in Pakistan; Port Cortes in Honduras; Southampton in the United Kingdom; Port Salalah in Oman; Brani Terminal at the Port of Singapore; the Gamman Terminal at Port Busan in Korea and the Modern Terminal at the Port of Hong Kong.

Southampton, Cortes, and Qasim meet the mandate of the SAFE Port Act, Sec. 232(b), to scan 100 percent of all U.S.-bound containers in three foreign ports. These three ports became fully operational on October 12, 2007. The additional four ports exceed the mandate of the SAFE Port Act and help to facilitate the compliance of the 9/11 Act, Sec. 1701(a), which demands that by 2012, all U.S.-bound containers must be scanned in a foreign port. By analyzing and reviewing SFI operations in these ports, DHS can better understand the unique challenges with 100 percent scanning at high-volume and transshipment ports.

In Phase I, DHS will provide the radiography equipment and DOE will install radiation portal monitors. DOE will also integrate the systems and provide the data to the foreign government at a Central Alarm System (CAS) where CBP will extract data on U.S.-bound containers and send to the National Targeting Center for analysis.

SFI sensor and image data gathered on containers bound for the United States will be encrypted and transmitted in near real-time to the U.S. Customs and Border Protection (CBP) officers working in overseas ports and to the DHS National Targeting Center. This data will be combined with other available risk assessment information to improve risk analysis, targeting and security of high-risk containers overseas.

Question 5. Under the SAFE Port Act, the DHS, working with the Commerce Department, is required to develop minimum performance standards for radiation scanning and non-intrusive imaging equipment capable of detecting WMDs within high-risk containers. What assurances does our Nation have that this equipment is capable of detecting weapons of mass destruction within high-risk containers? What actions has the agency taken to develop technological performance standards for scanning equipment, both domestically and at CSI ports? When do you anticipate finalizing the technological performance standards?

Answer. The Department of Homeland Security has taken great strides to ensure that all high risk containers entering our borders are screened. In addition, Customs and Border Protection (CBP) and the Domestic Nuclear Detection Office (DNDO) have devised a joint deployment strategy that seeks to deploy Radiation Portal Monitors (RPM) to all of our official ports entry. As of December 6, 2007, 100 percent of all incoming cargo on the Southern border is being scanned for the presence of radiological or nuclear material, nearly 98 percent at our seaports, and 91 percent on the Northern border. CBP and DNDO have confidence in the ability of the RPMs deployed to detect rad/nuc material and are working to develop and deploy a next-generation RPM, the Advanced Spectroscopic Portal (ASP) that will have the ability to not only detect the presence of material, but also identify the material.

In accordance with Section 121(f) of the SAFE Port Act, DNDO, in collaboration with the National Institute of Standards and Technology (NIST), shall publish technical capability standards for the use of NII and radiation detection equipment in the United States. Since Section 121(f) requires such standards to take into account relevant standards and procedures utilized by other Federal department or agencies as well as those developed by international bodies, NIST is presently conducting a study of the detection capabilities required by existing national and international consensus standards for radiological and nuclear detection.

Prior to deploying NII or radiation detection equipment, a complete site survey is conducted at the proposed site. During this survey port/terminal operators are encouraged to participate and provide input. All stakeholders are given the opportunity to provide input into final designs. Deployment activities do not commence until all stakeholder concerns and input have been addressed and satisfied.

Question 6. For good reason, much of our attention is focused on threats to maritime security posed by cargo container ships. But the possibility exists that terrorists may attempt to use oil tankers to stage an attack. Detecting a bomb in a tanker could be extremely difficult, if not nearly impossible. Most of these tankers are foreign flagged vessels filled up at foreign ports. How does the Administration view the potential for terrorists to use an oil tanker for a terrorist attack? To what extent have we considered this threat in planning for port security?

What agency has lead responsibility for examining or addressing this threat? Is it the Coast Guard? Is it the Navy? Overall, what efforts are being made to improve our security on this front?

Answer. Per the National Strategy for Maritime Security, the Department of Homeland Security, with the U.S. Coast Guard as its executive agency, has the primary responsibility for maritime homeland security. Additionally, per the Transportation System Sector-Specific Plan, the U.S. Coast Guard is the Sector Specific Agency (SSA) for the Maritime transportation mode. In these capacities, the Coast Guard has considered the potential for terrorists to attack oil tankers or other large vessels carrying high-consequence cargoes—either through external means (*i.e.,* waterborne IED attack) or an internal attack, such as a bomb on board. Port security planning does account for such scenarios. However, absent cueing intelligence, preventing such attacks presents significant challenges.

The Maritime Operational Threat Response (MOTR) process is significantly improving our national port security by integrating efforts among Federal, state and local partners. If cueing intelligence becomes available, the Coast Guard would exercise the MOTR process to engage other agencies as needed to ensure the vessel was located, intercepted, and boarded prior to approaching U.S. ports. If the threat were external, an armed escort would also be employed.

Absent cueing, the Coast Guard uses a risk-based methodology to identify which vessels to board prior to entry into a U.S. port. Many risk factors, including vessel characteristics, compliance history with domestic and international security regulations, information provided in the advance Notice of Arrival (NOA) report which lists the cargo carried, and intelligence information, are considered in selecting boarding candidates. Part of that security boarding process includes ensuring the vessel is under the control of the legitimate operators, and determining whether or not it is safe to allow entry into port. The boarding officer also makes recommendations to the Coast Guard Captain of the Port as to whether or not additional security measures are warranted. Such precautions might include armed vessel escorts (to protect against an external attack) and/or Positive Control Measures (retaining armed Coast Guard members aboard during the transit, to detect internal threats).

Beyond the above measures, the Maritime Transportation Security Act (MTSA) requires such vessels to have and maintain a Vessel Security Plan (including designation of a Security Officer), to have measures to address access control to critical spaces aboard the vessel and to regularly exercise the Plan. Such vessels are subject to both announced and unannounced Coast Guard spot checks and inspections to ensure compliance.

Question 7. As you know, to help secure the overseas supply chain, the Maritime Transportation Security Act required the Coast Guard to develop a program to assess security measures in foreign ports and, among other things, recommend steps necessary to improve security measures in those ports. Subsequently, the SAFE Port Act required the Coast Guard to reassess security measures at the foreign ports every 3 years. If foreign ports or facilities fail to maintain effective antiterrorism measures, the Coast Guard may deny entry to vessels arriving from that port or prescribe conditions of vessel entry into the United States. The Fiscal Year 2007 DHS Appropriations Act provided sufficient funding to increase the rate of foreign inspections from a 5-year cycle to the required 3 year cycle. Is the Coast Guard suf-

ficiently staffed to conduct these international inspections required under the SAFE Port Act? Do you have the resources you need to fulfill this requirement, or are additional resources needed?

Answer. The Coast Guard is sufficiently staffed to conduct international assessments required under the SAFE Port Act. Additionally, the Coast Guard will be assessing security measures of U.S. trading partners every 2 years as required by the 2007 Department of Homeland Security Appropriations Act instead of every 3 years as required by the SAFE Port Act.

Question 8. Does the Coast Guard's rotation of personnel from position to position prevent the development of an experienced workforce for this inspection program? Does that policy serve as a possible hindrance for the success of the international inspections?

Answer. No. A training and qualification program exists to ensure personnel conducting the assessments can perform their duties. Furthermore, a cadre of civilian personnel provides experience and continuity for the program. Therefore, the rotation policy improves the Coast Guard's ability to perform the assessments as officers with fresh perspectives and a wide range of safety, security, and environmental protection backgrounds are constantly entering the program. Ultimately, this enhances the Coast Guard's ability to share best practices with the countries visited.

Question 9. It seems that this inspection program might make some countries feel like their sovereignty is threatened—particularly if the inspections are fairly frequent. Has the Coast Guard encountered resistance from foreign governments on this inspection program? If so, how have you dealt with this challenge?

Answer. The Coast Guard has encountered some reluctance, but no country has flatly refused to allow the Coast Guard to visit. The Coast Guard deals with this challenge in a variety of ways. First, we do not characterize visits as "assessments" but rather as country visits to exchange information and share best practices. The Coast Guard emphasizes to the host nation that sharing information can improve their security as well as that of the United States. Moreover, the Coast Guard has a cadre of International Port Security Liaison Officers stationed overseas who engage with the host country representatives to build relationships and trust. We also offer reciprocal visits with the host country partners to observe our security practices. Finally, the Coast Guard partners with the U.S. State Department's consular team to negotiate access, when necessary.

Question 10. Does the Coast Guard have a management plan for TWIC enforcement in place? What are going to be the additional resource requirements for TWIC enforcement? What do you see as the challenges in carrying out the mission? Does the Coast Guard intend to have FTEs dedicated to TWIC enforcement or are these individuals going to be tasked with multiple missions?

Answer. The Coast Guard has taken multiple steps to ensure TWIC enforcement, including producing a Concept of Operations governing Coast Guard enforcement of TWIC provisions, and updating the Coast Guard Law Enforcement Manual to incorporate TWIC. The Coast Guard is also in the process of producing TWIC enforcement policy guidance in the form of a Commandant Instruction. The Coast Guard intends to apply existing facility and vessel inspection personnel and leverage the capabilities of its law enforcement partners toward TWIC enforcement and does not currently expect to need additional resources for this specific enforcement mission.

As with all enforcement responsibilities, protocols and procedures on scope and enforcement discretion must continually be validated. In addition, the Coast Guard faces challenges with implementation of TWIC readers, including acquisition of readers that meet the newly developed specification. The TWIC readers will incorporate new technology which requires appropriate testing for operation in all environments to ensure performance does not delay commerce, vehicles, or workers.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. FRANK R. LAUTENBERG TO REAR ADMIRAL DAVID P. PEKOSKE

Question. How does this Administration intend to meet the requirements for getting top priority "interagency operations command centers" up and running by 2009? And how will this be done when the President had requested no funding for these projects next year?

Answer. In the last 3 years the Coast Guard has established four Sector Command Center-Joint (SCC–J) facilities which host interagency representation from other agencies such as Customs and Border Protection (CBP) and the U.S. Navy (USN). In the Coast Guard's FY 2008 budget both Rescue 21 (R21) and Nationwide

Automated Information System (NAIS) projects will provide critical capability to select Coast Guard Command Centers.

The Coast Guard and CBP established a senior guidance team in 2006. One of the work groups established evaluated joint Coast Guard/CBP operations center requirements and identified eight "best practices" being used in various ports. These were promulgated as guidelines for consideration by other local Coast Guard/CBP Sectors and Port Directors.

In cooperation with DHS S&T, the Coast Guard has conducted test programs in two ports (Miami and Norfolk) evaluating software applications to automate situational awareness of port activity for the Coast Guard and associated port partners. Both of these tests are on-going. The Coast Guard is also cooperating with the Department's SBINet program to ensure synergy whenever possible.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO MAURINE SHIELDS FANGUY

Question 1. I understand TWIC enrollment began in Wilmington, Delaware on October 16, and you have finally announced the next eleven locations. When can we expect to see the deployment schedule for the TWIC program at the other 134 enrollment locations?

Answer. On October 31, 2007, the Transportation Security Administration (TSA) released a general schedule for all 147 enrollment locations. TSA and the U.S. Coast Guard expanded the original list of 134 to 147 based on stakeholder input. This listing provides monthly or quarterly deployment time-frames. The TWIC table shown is available to the public on TSA's website at *www.tsa.gov/twic*.

TWIC Quarterly Deployment Plan

[As of November 20, 2007]

October–December 2007		January–March 2008		April–June 2008	July–September 2008
October 16, 2007	Wilmington, DE	American Samoa	Palm Beach, FL	Alpena, MI	Bridgeport, CT
November 1, 2007	Corpus Christi, TX	Anacortes, WA	Panama City, FL	Anchorage, AK	Burlington, VT
November 7, 2007	Baton Rouge, LA	Ashtabula, OH	Pittsburgh, PA	Bangor, ME	Chester, PA
	Tacoma, WA	Bay City, MI	Port Canaveral, FL	Benicia, CA	Eureka, CA
	Honolulu, HI	Bourne, MA	Port Everglades, FL	Camden, NJ	Evansville, IN
November 8, 2007	Oakland, CA	Buffalo, NY	Portland, OR	Chattanooga, TN	Houma, LA
	Beaumont, TX	Calcite, MI	Richmond, CA	Coos Bay, OR	Lafayette, LA
November 14, 2007	Houston,TX	Cincinnati, OH	S. Louisiana (La Place, LA)	Coram, NY	Lindenhurst, NY
	Providence, RI	Duluth-Superior, MN	Salisbury, MD	Freeport, TX	Longview, WA
November 15, 2007	Chicago, IL	Escanaba, MI	Sandusky, OH	Galveston, TX	New Castle, DE
	Port Arthur, TX	Everett, WA	Sault Ste. Marie, MI	Greenville, MS	Pasco, WA
	Savannah, GA	Green Bay, WI	St. Ignace, MI	Gulfport, MS	Pennsbury Manor, PA
November 21, 2007	Baltimore/Dundalk, MD	Guam	St. Louis, MO	Guntersville, AL	Perth Amboy, NJ
	Minneapolis, MN	Hilo, HI	Tampa, FL	Juneau, AK	Port Manatee, FL
	St. Paul, MN	Huntington, WV	Texas City, TX	LaPorte, TX	Riverhead, NY
	Lake Charles, LA	International Falls, MN	Toledo, OH	Little Rock, AR	Sacramento, CA
November 28, 2007	Charleston, SC	Jacksonville, FL	Traverse City, MI	Marcus Hook, PA	St. Croix, USVI
November 29, 2007	Cleveland, OH	Kahului, Maui, HI	Vicksburg, MS	New Haven, CT	St. Thomas, USVI
	Detroit, MI	Key West, FL	Victoria, TX	New London, CT	Stockton, CA
	Port Fourchon, LA	La Plata, MD	Wilmington, NC	Nikiski, AK	Vancouver, WA
November 30, 2007	Boston, MA	Lorain, OH		Paducah, KY	
December 5, 2007	Brownsville, TX	Louisville, KY		Paulsboro, NJ	
	Mobile, AL	Marine City, MI		Point Comfort, TX	
December 12, 2007	Brunswick, GA	Marquette, MI		Ponce, PR	
	Milwaukee, WI	Memphis, TN		Port Hueneme, CA	
December 13, 2007	Philadelphia, PA	Miami, FL		Portland, ME	
Mid December	Albany, NY	Morehead City, NC		Portsmouth, NH	
	Indiana Harbor, IN	Morgan City, LA		Rochester, NY	
	Long Beach, CA	Muskegon, MI		Saipan	
	Los Angeles, CA	Nashville, TN		San Diego, CA	
	Seattle, WA	New Orleans, LA		San Francisco, CA	
	Tulsa, OK	New York/New Jersey #2		San Juan, PR	
Late December	Joliet, IL	New York/New Jersey #3		Valdez, AK	
	Kansas City, MO	Newport News, VA			
	Kauai, HI	Norfolk, VA			
	New York/New Jersey #1	Ontonagon, MI			
	Peoria, IL	Oswego, NY			

As the start of the enrollment period for each grouping of ports nears, TSA will post a specific enrollment start date in the *Federal Register*. To date, TSA has announced the start of enrollment for 22 locations in the *Federal Register*.

Question 2. How many mobile enrollment stations has the TSA contracted to use in addition to the fixed enrollment stations? How are they being distributed throughout the country? How would an employer go about arranging for a trusted agent to enroll employees at their facility?

Answer. Currently there are approximately 100 mobile centers identified. Additionally, Lockheed has the ability to deploy additional resources based on enrollment surges and owner/operator demands. We will continue to evaluate the need for mobile centers throughout the program's deployment. Employers interested in arranging for a mobile enrollment center, should contact the Lockheed Martin Operations Manager, Stacy Bonnah-DeMoss at 703–310–9157, or the Field Coordinator to discuss arrangements at the requestor's facility.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO MAURINE SHIELDS FANGUY

Question 1. My understanding is that when the TWIC card reader becomes available and is deployed at ports, workers wanting to gain access to secure areas will have to present their finger to the card reader only when there is an elevated threat level—MARSEC LEVEL 2 and above. Is that the case? Since 9/11, how many occasions have ports been at MARSEC LEVEL 2 and above?

Answer. Currently there are no regulatory requirements pertaining to use of TWIC readers. However, initial testing and evaluation of TWIC readers is expected to begin during calendar year 2008 as part of pilot testing. Data from pilot tests will be used to inform the second rulemaking which will address use of readers aboard MTSA-regulated vessels and facilities.

Including 9/11, there have been 10 occasions of the Coast Guard setting MARSEC Level 2 or above.

Question 2. On a day-to-day basis, when a port is at MARSEC LEVEL 1, would a port only be validating that the TWIC card being presented is authentic but not that the TWIC card being presented actually belongs to the individual presenting it? Isn't the purpose of TWIC to authenticate the identity of the worker?

Answer. The purpose of the TWIC card is to authenticate the identity of the workers. Currently, there are no regulatory requirements pertaining to the use of TWIC readers. However, initial testing and evaluation of TWIC readers is expected to begin in calendar year 2008 as part of our pilot phase. Data from the pilot tests will be used to inform the second rulemaking which will propose regulations related to the use of readers aboard MTSA-regulated vessels and facilities.

Question 3. I am concerned that the deployment of a durable, reliable, cost effective contactless card reader that can work in a maritime environment is years away. In the meanwhile, if allowed to, I believe that some ports may choose to purchase card readers that do not have finger template matching capability, deploy these readers at most its gates, and only purchase one or two more expensive card readers with finger template matching capability. In the event of a MARSEC LEVEL 2, there would likely be a couple of chokepoints at a port, at a time it least can afford it. What can you do to ensure that ports will purchase and deploy card readers at all gates that can operate at MARSEC LEVEL 2?

Answer. Currently, there are no regulatory requirements pertaining to the use of TWIC readers. However, initial testing and evaluation of TWIC readers is expected to begin in calendar year 2008 as part of our pilot phase. Data from the pilot tests will be used to inform the second rulemaking which will propose regulations related to the use of readers aboard MTSA-regulated vessels and facilities. We are committed to striking an optimal balance between commerce and security and will strive to minimize disruption to seaport activities during periods of heightened alert.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO MAURINE SHIELDS FANGUY

Question 1. How many TWIC cards have been issued and activated as of today?

Answer. As of Friday, November 16, 2007, there have been 4,574 enrollments and 1,061 credentials activated.

Question 2. How many TWIC card readers are in place as part of the pilot program?

Answer. One of the main purposes of the pilot is to configure readers for contactless reading of a Transportation Worker Identification Credential card. We anticipate having these in place in the early 2008 time-frame.

Question 3. I understand that ports which are testing new TWIC card readers as part of a TSA pilot program are being required to use their port security grant funds to do so, and must pay for 25 percent of the cost. Why doesn't TSA pay for the entire amount of testing? I understand TSA has authority to waive the cost share requirement under the port security program. Do you intend to do this?

Answer. The Security and Accountability For Every Port Act of 2006 (SAFE Port Act) instructed the Department of Homeland Security to conduct a pilot program to test the business processes, technology, and operational impacts required to deploy transportation security card readers at secure areas of the marine transportation system. The overall Transportation Worker Identification Credential (TWIC) program and this TWIC Pilot Program are managed by TSA. However, the Pilot Program is funded through the Port Security Grant Program (PSGP); therefore all of the requirements of PSGP must be met, including the 25-percent match. TSA does not have the authority to waive the cost share requirement under PSGP. Pursuant to 46 U.S.C. 70107(c)(2)(b), only the Secretary of Homeland Security has the authority to waive this requirement. Waiver requests for these projects have been submitted to the Secretary and are being reviewed.

Question 4. What progress has your agency made in establishing a system to ensure that 100 percent of all incoming containers are scanned for radiation before being shipped to our shores?

Answer. Lessons learned from the initial deployment of the Secure Freight Initiative (SFI) will assist CBP in meeting this requirement in a practical and measured manner, and in a way that does not adversely affect global trade. On October 12, 2007, Southampton, United Kingdom; Port Qasim, Pakistan; and Puerto Cortez, Honduras became the first fully operational seaports to implement SFI. These ports fulfill the requirements set out in the Security and Accountability For Every Port Act of 2006, (SAFE Port Act) which establishes a program that couples Non-Intrusive Inspection (NII) and radiation detection technology. At these three ports, all maritime containers destined for the United States are scanned using radiation detection and imaging equipment. Data from these systems is then provided to U.S. officials at U.S. Customs and Border Protection's National Targeting Center for analysis.

Four additional ports will become operational for Phase I of the project and will provide scanning on a limited capacity basis: Singapore's Brani terminal; Busan, Korea's Gamman terminal; Hong Kong's Modern Terminal; and Salalah, Oman. DHS, Department of Energy's National Nuclear Security Administration (NNSA) and Department of State, partnered with these ports because they pose different challenges and provide diverse environments in which to evaluate various options. Specifically, these ports will help to elucidate how effective and efficient 100 percent scanning can be in high-volume and transshipment ports.

A report is due to Congress in April 2008 on the status of 100 percent scanning abroad. DHS continues to develop and refine the metrics used to define the success and challenges of the SFI program in the selected ports. As the recently passed 9/11 Act requires 100 percent scanning by 2012, the information contained in this report will be critical in determining an appropriate and responsible path forward for SFI.

Question 5. When will TSA complete threat assessments for port truck drivers, as required by Section 125 of the SAFE Port Act of 2006?

Answer. The Transportation Security Administration (TSA) anticipates completion of the threat assessments for port truck drivers by summer 2008. Collection of driver information from all state motor vehicle licensing agencies is underway at this time. There is substantial variation in the technological capabilities of the states, leading some to respond to TSA's request earlier than others. Also, as the Transportation Worker Identification Credential is deployed across the country we will enroll these drivers and they will go through a much more thorough check than the name-based check, which will be done perpetually.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO HON. THOMAS S. WINKOWSKI

Question 1. Based upon your experience to date with the development of the pilot program to test integrated scanning systems in three foreign ports, what have you found to be your major obstacles? What costs has the Federal Government incurred to implement this pilot program?

Answer. The success of the Secure Freight Initiative (SFI) pilots in Qasim (Pakistan), Cortes (Honduras), and Southampton (UK) illustrates that scanning all U.S.-bound maritime containers in a foreign port is feasible on a relatively contained scale. However, successfully deploying container scanning equipment in these three ports and establishing SFI in the four limited capacity ports (Hong Kong; Singapore; Busan, Korea; and Salalah, Oman) has presented certain technological, logistical and diplomatic challenges, such as the following:

- Re-configuring port layouts to accommodate the equipment without affecting port efficiency;
- Addressing health and safety concerns of host governments and respective trucking and labor unions;
- Ensuring the sustainability of the scanning equipment in extreme weather conditions and certain port environments in third-world countries;
- Determining who will incur the costs for operating and maintaining the scanning equipment;
- Developing local response protocols for adjudicating alarms;
- Varying costs of transferring the data back to the United States (National Targeting Center) in real-time, etc.;
- Addressing data privacy concerns in regards to the scanning data;
- Concluding arrangements with partnering nations and terminal operators that may own and operate the scanning equipment;
- Staffing implications for both the foreign customs service and terminal operator;
- Licensing requirements for the scanning technology; and
- The potential requests for reciprocal scanning of U.S. exports as a condition for a country's cooperation in SFI.

Thus far, becoming fully operational and negotiating SFI implementation has cost the Department of Homeland Security (DHS) $30,445,126.83. The breakdown of costs is as follows:

CBP Cost Element	
Analytical Study	$200,000.00
Communications	$2,709,878.76
Equipment	$10,155,000.00
Hardware	$2,996,193.51
Hardware (server license)	$82,131.68
Port Deployment Support	$463,923.00
Program Office Support	$1,657,500.00
Software Development	$10,080,883.71
Software License	$628,485.93
Software Support	$140,535.29
Training	$231,502.36
Travel	$1,099,092.59
Total	$30,445,126.83

Through FY 2007, the National Nuclear Security Administration has spent a total of $29.3 million to implement SFI. The breakdown is as follows:

Equipment	
RPMs	$1,468,289
ASPs	$368,194
RIIDs	$862,220
MRDIS	$1,863,750
OCR	$350,000
Handhelds	$134,304
Total Equipment	$5,046,757
Installation Total	$17,278,581
Communication Total	$5,935,582
Testing Total	$465,000
Maintenance Total	$550,000
Grand Total Expenditures	$29,275,920

Question 2. What actions have you taken to satisfy the 100 percent domestic scanning requirement in the SAFE Port Act for the top 22 U.S. ports? Are you currently in a position to meet the deadline of December 2007? What complications have you experienced to date and what steps are you taking to address these complications?

Answer. RPMs were commissioned at San Diego and Tioga during December of 2007, completing all planned RPM deployments for the top 22 U.S. ports by the end of Calendar Year 2007. With these deployments, U.S. Customs and Border Protection (CBP) now scans greater than 97.3 percent of all seaport containerized cargo.

Complications experienced were associated with intermodal terminals which use straddle carriers to transport containers to rail. These terminals (Maher in Elizabeth, New Jersey; PCT, T–4 and T–7 in Tacoma, Washington; and West Palm Beach in Florida) account for approximately 2.1 percent of all container volume entering the United States. The current technology solutions cannot screen cargo transported by straddle carriers. Hence they have been deferred pending a new solution. CBP is working with the Domestic Nuclear Detection Office on this solution.

Question 3. Although recommended by the GAO and required by the SAFE Port Act, minimum technical operating standards for non-intrusive inspection equipment at CSI ports have yet to be established. What assurances does our Nation have that this equipment is capable of detecting weapons of mass destruction within high-risk containers?

What actions has the agency taken to develop technological performance standards for scanning equipment, both domestically and at CSI ports? When do you anticipate finalizing the technological performance standards? What assurances does our Nation have that this equipment is capable of detecting weapons of mass destruction within high-risk containers?

Answer. Through the Container Security Initiative (CSI), U.S. officers work with host customs administrations to establish security criteria for identifying high-risk containers. With the establishment of security criteria, CBP has benefited in our ability to identify high-risk containers for terrorism and also by the information received when the host government conducts examinations. Prior to CSI, many of these customs administrations were not using non-intrusive imaging (NII) technology to inspect the high-risk containers before they were shipped to U.S. ports. With the establishment of CSI, the host government administrations of the 58 CSI operational ports have invested millions of dollars on NII equipment and have also purchased their own radiation detection devices to include Radiation Portal Monitors to use as part of their examination process. Consequently, the level of examinations conducted at CSI locations increased by 93 percent from 70,902 in Fiscal Year (FY) 2006 to 136,815 in the FY 2007. These increased levels of workload resulted in an array of enforcement actions and investigative cases. This level of success could not have been accomplished without the host government continued cooperation and the resulting effective examination process.

Host government officials have not hesitated in providing CBP with all the information derived from equipment used for the inspection of containers. This equipment is equal to or better than the equipment used by CBP at its domestic ports. CBP officers are fully trained in the equipment being used by the host government,

and in the cases where CBP has provided NII equipment, those host government customs officers have also been trained in the use of that equipment.

In addition to this, CBP, through its Capacity Building Branch within the Office of International Affairs and Trade Relations, is providing training and technical assistance to the customs administrations of a number of countries that currently participate in CSI, including Brazil, Honduras, the Dominican Republic and South Africa. This training and technical assistance forms a long-term capacity building program to support implementation of the World Customs Organization Framework of Standards to Secure and Facilitate Global Trade. The standards incorporated into the Framework incorporate many of the key elements which support CSI including: the advance electronic presentation of cargo information; the screening of cargo containers using non-intrusive inspection equipment; the use of automated risk management systems; the standardization of targeting criteria to identify high-risk cargo and containers; an emphasis on employee integrity programs; and the inspection of cargo in the country of origin, transit and destination.

CBP's Training and Assistance Division of the Office of International Affairs and Trade Relations currently provides a number of assistance and training programs to foreign customs and border security agencies to facilitate implementation of port security antiterrorism measures. Through its Capacity Building program in support of the World Customs Organization Framework of Standards to Secure and Facilitate Global Trade, CBP provides a long-term training and technical assistance program to partner customs administrations that includes an in-depth assessment of its seaport security practices.

Question 3a. What actions has the agency taken to develop technological performance standards for scanning equipment, both domestically and at CSI ports?

Answer. Domestically for imaging systems, CBP uses American National Standards Institute (ANSI) and the Occupational Safety and Health Administration (OSHA) radiation standards and other Federal standards, such as the National Fire Protection Association's (NFPA 79), Electrical Standards for Industrial Machinery to procure NII equipment. CBP is presently using the Draft Standard for Determination of the Imaging Performance of X-Ray and Gamma-Ray Systems for Cargo and Vehicle Security Screening, IEEE PN42.46/D1 dated July 2007, prepared by the Cargo/Vehicle Working Group of the National Committee on Radiation Instrumentation N42 Committee. Draft Standard is in final stages of approval.

For radiation portal monitors (RPM), CBP uses the technological performance standard ANSI N42.35 standard for the Polyvinyltoluene (PVT) radiation detection technology and the N.42.38 standard for the Advanced Spectroscopic Portal technology.

CBP worked with a number of agencies to define and specify the performance requirements for radiation scanning, resulting in the Department of Energy threat guidance for radiological materials document. The development of this standard used a number of CBP inputs:

1. Types of conveyances to be scanned (automobiles, commercial vehicles, containers, etc.) for radiation.

2. Types of cargo that are imported that may provide shielding of the radiation.

CBP then used the performance requirement to identify, procure, and validate the detection capability of systems to deploy.

1. Used Request for Information (RFI) to determine the capability of existing equipment to meet the CBP requirements.

2. Purchased and evaluated several manufacturers of radiation detection equipment.

3. Used the RFI and evaluation information to develop procurement specifications that pushed the limits of commercial off the shelf (COTS) equipment.

4. Issued Request for Proposals (RFPs) to viable manufacturers of radiation portal monitor type equipment.

5. Awarded a single competitive contract (based on pricing) for the first generation (PVT-based) radiation portal monitors.

6. Verified the systems meet the CBP requirements through a series of factory and government acceptance tests, supplemental testing at a national laboratory, and field validation in a CBP port.

CBP also developed a process for establishing NII technological performance standards that are based on current industry capabilities and will accommodate future technology advances. To develop these technological performance standards CBP has taken the following actions:

- Identified the types of containers (*e.g.,* automobiles, trucks, railcars, sea containers) that must be penetrated to scan the commodities within the containers.
- Used CBP's commodities list that contains the type, volume and density of commodities entering the United States to determine the penetration, contrast sensitivity and resolution needed to detect illicit materials.
- Used Research and Development (R&D) capabilities as input to develop the initial baseline for operational requirements.
- Issued RFIs to determine latest industry capabilities to meet or exceed CBP requirements.
- Used RFI responses to update initial technology performance requirements.
- Issued RFPs to vendors that could meet or exceed CBP performance requirements for penetration, contrast sensitivity, resolution and environmental needs.
- Included provisions for vendors to provide the government with the most current technology and the ability to offer technology refreshments in the future.
- Awarded an Indefinite Delivery/Indefinite Quantity (IDIQ) contract to five vendors to compete and provide NII equipment that satisfied performance specifications for penetration, contrast sensitivity, resolution and throughput; and other requirements such as the North American Train Bridge Envelope for height and width requirements, image quality, controlled operating area footprint, and environmental requirements for operating in −20 °F 120 °F.
- Under a DHS approved Test and Evaluation Master Plan (TEMP), CBP performs government acceptance testing on all domestic and CSI NII equipment procured under the CBP IDIQ contract to include Government Factory Tests and Site Acceptance Tests to insure all performance standards and requirements are met.

For CSI ports, CBP has submitted the United States' "Declaration of Intent" to adopt the World Customs Organization "Framework of Standards to Secure and Facilitate Global Trade." This international strategy will combat terrorism and protect trade and the global economy.

The framework incorporates key elements of the U.S. strategy for securing trade and harmonizes certain customs standards and procedures among World Customs Organization members that implement the framework. These key elements are based in large measure on initiatives, systems and processes designed and implemented by CBP—including the CSI program, the "24-Hour Rule", the Automated Targeting System and the Customs-Trade Partnership Against Terrorism (C–TPAT).

Core elements of the framework are: harmonization of advance electronic manifest requirements on inbound shipments; outbound transit shipments; a standard approach to risk management; inspection of outbound cargo using non-intrusive detection equipment; and providing tangible benefits to businesses that meet minimum supply chain security standards and implement best practices. CBP has further recommended that its counterparts in host nations purchase NII systems that follow the guidelines on page 10 of the World Customs Organization, Customs Compendium, Container Scanning Equipment, Guidelines to members on administrative consideration of purchase operation.

Question 3b. When do you anticipate finalizing the technological performance standards?

Answer. As stated above, CBP has continued to recommend that its counterparts in host nations purchase NII systems that follow the World Customs Organization Compendium and has incorporated this language in all Declarations of Principles that were signed by all new participants to the CSI Program, beginning with Portugal (July 2005).

Question 4. Section 204 of the SAFE Port Act required that CBP establish standards for cargo locks and seals. When can we expect these standards to be finalized?

Answer. On May 18, 2007, the DHS notified Congress of its decision not to initiate a rulemaking proceeding to establish minimum standards for securing containers in transit to the United States within the mandated timeline. DHS readily acknowledges that the process of securing the container is a critical component of a multilayered strategy to secure the entire supply chain. However, DHS does not believe, at the present time, the necessary technology exists for such a solution.

The CBP-developed Conveyance Security Device system and component technical requirements were published in a RFI on December 12, 2007.

DHS policy concerning applicability and use will be determined when an acceptable device(s) is approved.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO HON. THOMAS S. WINKOWSKI

Question 1. In my state there are both public and private ferries that operate between cities in Washington and points in Canada. Immigration clearances are performed in Canada prior to the passenger departing, but the customs declaration and clearance is performed in the U.S. The SAFE Port Act gave DHS 120 days to develop a plan for the inspection of passengers and vehicles in ferries bound for the U.S. before the vehicles and passengers are loaded onto the vessel. It makes sense to co-locate the immigration and customs declarations function and perform them prior to when the ferry departs for the U.S. When should the committee expect to receive the Department's plan?

Answer. CBP advised that they have completed the review and currently pursuing developing a plan as required by section 122 of the SAFE Port Act. Additionally, CBP reached out to ferry owners and operators to gauge their interest in a ferry pre-clearance process. Those owner/operators that provided comments at this early stage were very adamant that any procedures developed by CBP should not include cost to be borne by the ferry owners/operators.

In order to move to "full preclearance" in Victoria whereby immigration, customs, and agricultural missions are conducted at one site, the infrastructure in Victoria must be upgraded. Each of the three facilities in Victoria are dated, lack adequate space for efficient inspections and vehicle queuing, and offer limited administrative workspace to CBP officers. The Province of British Columbia and the Sea Ferry Operators themselves have been reluctant to fund the improvements necessary to move to "full preclearance." It is CBP's position that the Province and/or the Sea Ferry operators are responsible for adequate facilities.

CBP has similar concerns about implementing such a process in other ferry locations as well. Foreign governments and the private sector have indicated a reluctance to fund security enhancements that they view as solely beneficial to the U.S. Government. In addition, there are sovereignty concerns that arise when negotiating with Canada and other countries on such issues. The countries—Canada, Mexico, Dominican Republic, and the UK (British Virgin Islands)—are concerned about the resource implications as well as whether their officials would be granted similar authorities within the United States. There is also a concern that further pursuit of this initiative could make future attempts at cooperation on other homeland security matters more difficult and undermine our ability to provide the types of services currently underway.

Question 2. A number of my constituents living in Whatcom, Skagit, and Snohomish counties own or rent boats, and take weekend or in some cases daily trips to Canada. Until the beginning of 2006, the state had seven customs points of entry. Subsequently, the ports of entry in the Cities of Bellingham and Everett were dropped. Unless you live out there or visit these communities it may be hard to understand why this is such a big deal. Do you know why the two custom ports of entry were closed? How was this decision disseminated to the affected communities? Are the closures the result of lack of available staffing resources?

Answer. As of January 1, 2006, pleasure boaters in Puget Sound have been restricted to reporting for face-to-face inspections at five (5) designated Puget Sound locations. The five (5) locations are strategically located at the north and east entryways into the Sound: Point Roberts, Friday Harbor, Roche Harbor, and Anacortes to the north, and Port Angeles to the east.

Historical records support the restriction to the above locations, with the majority of boaters arriving at Friday and Roche Harbors. The strategy provides CBP with an improved enforcement posture in the pleasure boat arena. Boaters arriving from foreign locations may still call on other ports within the Sound for clearance. However, they must make appointments in advance. Boaters who have not stopped at a designated location and do not have an appointment for clearance at another port may be subject to penalty.

The boating community was notified via press release and flyers of the change to designated ports for processing. Flyers were distributed at boat shows and outreach was conducted to include boat clubs, marinas and a northwest boater magazine to maximize notification.

To reduce the number of potential face-to-face inspections that are required for pleasure boaters within this area, the Seattle Field Office implemented a strong campaign during FY 2005 to register boaters into the Canadian Border Boat Landing Permit Program (I–68). Approved participants must pass enforcement checks and an interview process. Once approved, participants are allowed to phone-in arrivals *in lieu of* meeting with a CBP officer, unless otherwise directed. Participation in NEXUS, a bilateral program with Canada, also provides boaters the privilege of

phoning in arrivals by boat. This program also requires an applicant to go through enforcement checks and interviews by both Canada and U.S. officers prior to acceptance into the program.

Question 3. I have heard from several ports in my state that when considering proposals to submit to the Port Security Grant program, port personnel focus on the proposed project's total life cycle costs in addition to the up front acquisition costs. They tell me that sometimes the best ideas do not go forward because the Port Security Grant program does not cover the operation and maintenance of systems obtained under the grant. Is it the case that the Port Security grant program does not cover operation and maintenance costs? Have any ports discussed with the agency concerns over the lifecycle costs for systems acquired with Port Security grant funds?

Answer. Since FY 2006, the cost of acquisition, operation, and maintenance of security equipment or facilities to be used for security monitoring and recording, security gates and fencing, marine barriers for designated security zones, security-related lighting systems remote surveillance, concealed video systems, security vessels, and other security-related infrastructure or equipment that contributes to the overall security of passengers, cargo, or crewmembers are allowable. In addition, routine maintenance costs for security monitoring, such as the cost of tapes for recording, have been allowable. However, these O&M costs are only allowable during the award period and business operations and maintenance costs, such as personnel costs and items generally characterized as indirect or "overhead" costs, are unallowable.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO HON. THOMAS S. WINKOWSKI

Question 1. Since the 2006 Inspector General report on the Automated Targeting System, what has your agency done to take advantage of other sources of intelligence information, or even commercially-available data to better screen potentially dangerous cargo?

Answer. CBP integrates intelligence information into ATS for the targeting and identification of high risk cargo utilizing a variety of methods. This information is vetted and integrated into ATS as a system rule or as part of a weight set to include national lookouts.

The CBP Office of Intelligence and Operations Coordination (OIOC) reviewed and updated the ATS National Security weight sets for ocean, air and truck (Northern and Southern) cargo during 2007. These weight sets are utilized by CBP to provide threshold targeting for national security risks utilizing ATS. OIOC worked with the Office of Field Operations (OFO) to implement the Auto Hold Event program in the ocean environment. Shipments scoring above the ATS National Security threshold in the ocean environment are automatically placed on hold by ATS for further review, vetting, and possible examination by CBP field personnel.

In 2007 OIOC developed, analyzed and implemented an updated "Country of Interest" list for security cargo targeting in ATS based on the analysis of intelligence reports and external data sources. OIOC continually utilizes information from the intelligence stream to create and update Weapons of Mass Destruction (WMD), Weapons of Mass Effect (WME), and conventional weapons rules in ATS. OIOC personnel monitor updates to Entity list designations made by the Office of Foreign Asset Control (OFAC) for extraction and upload into ATS.

OIOC has worked with personnel from Other Government Agencies (OGA) to create and update ATS Weight sets utilized by OGA responsible for targeting and intercepting cargo for security and terrorism threats. OIOC created a weight set for the U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service (APHIS) personnel responsible for targeting shipments in ATS posing a threat for agro-terrorism risk. This included the integration of an APHIS identified "Country of Interest" list and plant and animal disease tables. OIOC also created an ATS weight set for Food Safety and Inspection Service (FSIS) personnel in order to target importations (*i.e.,* ensuring that the Nation's commercial supply of meat, poultry, and egg products is safe, wholesome, and correctly labeled and packaged).

CBP is testing the capability for field users to create independent rules and rule sets (User Defined Rules). User Defined Rules (UDR) functionality for the creation of National Lookouts has been incorporated into ATS to ensure information received in intelligence stream and through operations conducted by CBP can proactively be added. CBP utilizes real time information gathered from CBP Intelligence, Law Enforcement Entities, OGA and other foreign governments for incorporation in ATS rules, weight sets and specific entity lookouts on a continuous basis to ensure threat

assessments are properly communicated for incorporation in national security targeting. Following a maritime transportation security incident, CBP currently has the ability to modify or create rules and incorporate specific "Look Outs" for identified national or local targeting threats. CBP has implemented functional and performance testing of ATS system rules, weight sets, and targeting elements employing these transactions in order to monitor and evaluate overall strategic targeting performance.

Commercial Available Data

CBP has initiated several efforts to acquire additional data sources to enhance the targeting of high risk cargo. CBP has two commercial databases: ChoicePoint (AutoTrack) and Accurint (Lexis-Nexis). In 2006, OFO revaluated the utilization of the ChoicePoint application, obligated funding and established a National ChoicePoint account for appropriate field personnel. In November 2005, the Accurint Commercial Database account was established. The Accurint account is maintained by DHS/CBP/OFO.

ChoicePoint is a commercial database that allows approved users to search over seventeen billion current and historical records for comprehensive research on individuals and businesses. Users can cross-reference public and proprietary records, including identity verification, information on relatives and associates, corporate information, real property records and deed transfers utilized to identify and manage risk and to detect anomalies.

Accurint is a commercial database that provides a full site of investigative tools that enable approved users to locate people, detect fraud, uncover assets and verify identity by providing instant electronic access to a comprehensive catalog of public records and non-public information. Accurint provides up to date information linking more than one hundred thirty-two million individuals, businesses, addresses and phone numbers.

CBP has initiated several efforts to acquire additional data sources to enhance the detection and resolution of significant manifest anomalies, including Dunn and Bradstreet, outbound U.S. Post Office data and Electronic Notice of Arrival (eNOA) data from the U.S. Coast Guard.

Importer Security Filing and Additional Carrier Requirements

CBP's 'Importer Security Filing and Additional Carrier Requirements' notice of proposed rulemaking (NPRM) was published in the *Federal Register* on January 2, 2008. The NPRM will be available for public comment until March 18, 2008. At the conclusion of the comment period, CBP will carefully study and consider the recommendations it receives before drafting a final rule. After the final rule is published, CBP will provide the trade ample opportunity to reconfigure their automated systems, normally 90 days, after which, the final rule will go into effect. Once the final rule is in effect, CBP plans to work with the trade during a 1-year informed compliance implementation period.

The onus of the new "10+2" data requirements rests upon the importers and vessel carriers, and not the overseas shippers. The *importer or his agent* will be responsible for filing the complete, accurate, and timely importer elements of the Security Filing. For the purposes of the proposed regulations, importer means the party causing goods to arrive within the limits of a port in the United States.

Under the proposed "10+2" regulations, *carriers* would be required to submit a *vessel stow plan* and *container status messages* regarding certain events relating to containers loaded on vessels destined to the United States.

OIOC is currently working with OFO to further develop the ATS Graphical User Interface (GUI) for display of the Security Filing data elements in ATS and the development and creation of additional targeting rules to identify high risk cargo shipments in the ocean environment based on these elements.

Question 2. How has DHS implemented Section 203 of the SAFE Port Act of 2006?

Answer. The requirements of section 203 of the SAFE Port Act are as follows:

Section 203

In General

Section 203 of the SAFE Port Act requires the Secretary, DHS, acting through the Commissioner of U.S. Customs and Border Protection, to identify and seek the submission of data related to the movement of a shipment of cargo through the international supply chain and to analyze the data received to identify high risk cargo for inspection. The Commissioner shall require the electronic transmission of advanced information in the form of additional data elements that he determines are necessary to improve the high risk targeting of U.S.-destined commercial cargo prior to its lading at a foreign seaport.

Additional Data Elements for Improved Targeting of High-Risk Cargo

Consideration shall be given to the cost, benefit and feasibility of: (A) requiring additional non-manifest 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 that the Secretary considers beneficial for improving the Automated Targeting System or any other targeting system in furthering the security and integrity of the international supply chain. In addition, the Commissioner shall consult with stakeholders, including the Commercial Operations Advisory Committee (COAC), and identify to them the need for such information, and the appropriate timing of its submission and the Secretary shall promulgate regulations to implement any changes made under Section 203.

Improvement of the Automated Targeting System

With regards to the Automated Targeting System (ATS), the Secretary, acting through the Commissioner, shall: (1) conduct an independent review of the ATS that evaluates the effectiveness and capabilities of the systems; (2) consider future iterations of the system that would incorporate smart features, complex algorithms and real time intelligence; (3) ensure that the system has the capability to electronically compare manifests and detect and resolve anomalies in the data; (4) ensure that the ATS has the capability to electronically, identify, compile and compare select data elements for cargo entering or bound for the U.S. following a maritime transportation security incident in order to identify cargo for increased inspection or expeditious release; and (5) address 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. Finally, all submission of information under these requirements are to be transmitted in secure fashion.

Section 203 Implementation

Acquiring Additional Data Elements for Improving the Targeting of High-Risk Cargo

To improve its ability to target high-risk, ocean-borne containerized and breakbulk cargo, CBP published a notice of proposed rulemaking (NPRM) on January 2, 2008, which would require importers and carriers to submit additional data. As proposed, this data would include:

- The Importer's 10 (I–10): Ten new pieces of information (four of which currently appear on the Entry) filed by the Importer 24 hours prior to the container being laden on a U.S.-bound vessel.
- The Carrier's 5 (C–5): Five new pieces of information based on the I–10 where there is no U.S. importer of record (*e.g.,* cargo that is for Immediate Export or Transportation and Export, and Foreign Cargo Remaining on Board filed by the Carrier, acting as the constructive Importer) prior to the container being laden on a U.S.-bound vessel.
- The Stow Plan: The vessel stow plan showing the vessel cargo configuration (as well as identifying and listing the actual containers aboard a vessel) after leaving the last foreign port bound for the United States, filed by the Vessel Operating Carrier 48 hours after departure (or prior to arrival for short haul legs). The stow plan and container list will be vetted against the manifested container list to identify any unmanifested containers electronically prior to vessel arrival.
- Container Status Messages: Messages in regard to lifecycle container events (*i.e.,* actual physical container movements), filed daily by the responsible carrier for all of its containers en route to the United States.

CBP proposed the additional data elements after a thorough consultation with the COAC and Trade Support Network. During this consultation, CBP communicated the need to have access to additional data elements for targeting purposes, and the trade community had an opportunity to express its concerns, such as the security of the data. The consultation was conducted in conjunction with an independent internal review which included targeting and field representatives as well as trade experts. This process resulted in the selection and, in the case of the I–10 and C–5, refined definition of the additional data, which CBP determined would add the most critical value to its targeting operations without impeding the flow of legitimate commerce. The security of the data is not an issue as the proposed submission methods for the I–10 and the C–5 are based on current secure transmission methods (Automated Broker Interface and Automated Manifest System). Further, the carriers have requested the ability to use Secure File Transfer Protocol (SFTP) or e-mail for submitting stow plans and sFTP for Container Status Messages.

Complying with SAFE Port Act Section 203(e), in August 2006, the DHS Office of Inspector General (DHS OIG) conducted a review of CBP Automated Commercial Screening and Targeting Release (OIG Report OIG–06–56). In November 2006, Sentinel HS conducted an independent review of the effectiveness and capabilities of CBP Automated Targeting System maritime targeting. In November 2006, the DHS OIG conducted a second review of Targeting for Oceangoing Cargo Containers (OIG Report OIG–07–09). Additionally, in September 2007, DHS OIG conducted a third review of Targeting Oceangoing Cargo Containers (OIG Report OIG–07–72).

In February 2006, CBP entered into a partnership with the S&T Directorate's Homeland Security Advanced Research Projects Agency (HSARPA) to explore the application of advanced analytical tools in the cargo-targeting environment to assess the incorporation of additional smart features into ATS. Three projects are underway to help CBP to develop predictive modeling, anomaly detection, and visualization tools that are customized to specifically analyze CBP cargo data. In addition to this effort, the CBP Deputy Commissioner established several work groups—comprised of CBP/OFO staff, Office of Information and Technology (OIT) personnel, Office of Anti-Terrorism staff, statistical analysts, and intelligence analysts—charged with using the historical findings, transactional data, and intelligence to investigate the feasibility of statistically calibrating the maritime security rules in December 2006. Other foci of the groups were to identify the creation of new optimized groups of rules and discovery of new rules. This group produced a presentation to the Deputy Commissioner and Assistant Commissioner of OFO, outlining the findings of the study and recommending potential changes to rules and weight sets. CBP OIT and HSARPA are exploring the applicability of the following advanced analytical tools in cargo targeting: Signature Analyst Automated Screening and Targeting Tool, Predictive Visual Analytics for Significant Encounters, and Shipping Container Anomaly Detection and Classification.

ATS currently has the capability to electronically compare manifest and other available data to detect any significant anomalies and facilitate their resolution. ATS has the capability to filter on all manifest, entry, and entry summary data elements. Through this mechanism, shipments can be identified as meeting particular risk criteria and can be targeted for increased scrutiny or for expeditious release. This capability includes manifest and entry data matching to Treasury Enforcement Communications System (TECS) records, D&B records, and to data provided by other government agencies (Food and Drug Administration, U.S. District Attorney, U.S. Coast Guard, Department Of Energy).

Following a maritime transportation security incident, CBP currently has the ability to modify or create rules and incorporate specific "Look Outs" for national or local targeting. CBP has also recently tested a capability for users to create independent rules and rule sets (User Defined Rules). This functionality provides the ability for users to more easily implement future anomaly rules. Additionally, CBP has initiated several efforts to acquire additional data sources to enhance the detection and resolution of significant manifest anomalies: Outbound Post Office data and eNOA data from the U.S. Coast Guard. As of FY 2007, CBP has incorporated the creation of mock shipments in the CBP Mock Shipment Environment in order to review the overall performance of automated targeting system rules for risk management validations. To date, over 25,000 mock shipments that include bill of lading and entry transactions have been created for performance evaluation of rules in the ocean environment. The process includes the formalization of weight set performance evaluation criteria, processes, and reporting. CBP has implemented functional and performance testing of ATS system rules, weight sets, and targeting elements employing these transactions in order to monitor and evaluate overall strategic targeting performance.

The OFO Audit Program Liaisons (APL) has established a uniform policy and procedures for the Government Accountability Office (GAO), OIG, and Internal Affairs Management Inspection Division (MID) audit process within OFO. OFO APL responsibilities include audit activities, reports, and corrective action plans. In addition, the CBP Office of Executive Secretariat (OES) inputs OFO recommendations in CBP's electronic project management system, to track and monitor entries and notify OES of any changes.

Question 3. During your testimony before the Committee, you indicated DHS/CBP obtains various data and content from sources for targeting of oceangoing cargo destined to the United States via the Automated Targeting System. Which data sources do you utilize? Which, if any, of these sources are not owned or controlled by the Federal Government? How do you envision the so-called "10+2" advance data rule integrating into the current targeting environment?

Answer. CBP obtains various data and content about oceangoing cargo destined for the United States from numerous sources throughout the supply chain life-cycle.

The two most common sets of information are the cargo manifest and the entry documentation. Both of these sets of information are provided to CBP electronically through CBP's Automated Commercial System (ACS). ACS is owned and controlled by CBP.

Currently, the data that CBP relies upon to do its advance targeting *prior to vessel loading* is, for the most part, the carrier's manifest information. While this was a sound initial approach to take after the tragic events of September 11th, internal and external reviews have concluded that more complete advance shipment data would produce more accurate, and therefore more effective cargo risk assessments.

The 'Importer Security Filing and Additional Carrier Requirements', also known as the "10+2 Security Filing" for which the NPRM was published in the *Federal Register* on January 2, 2008, would significantly enhance our targeting and risk analysis capabilities by increasing the transparency of key supply chain participants, identifying actual cargo movements, and improving the accuracy of cargo descriptions.

In addition, "10+2" would vastly improve the facilitation of lawful international trade by identifying low-risk shipments much earlier in the supply chain, thus reducing the need for a more thorough physical screening.

The NPRM is specifically intended to fulfill the requirements of section 203 of the SAFE Port Act of 2006 and section 343(a) of the Trade Act of 2002, as amended by the Maritime Transportation Security Act of 2002. The SAFE Port Act requires the Secretary of Homeland Security, acting through the Commissioner of CBP, to promulgate regulations to require the electronic transmission of additional data elements for improved high-risk targeting, including appropriate security elements of entry data for cargo destined to the United States by vessels prior to loading at foreign seaports.

Current Data

1. All cargo *shipments* heading into the United States must be properly manifested. A shipment is a movement of cargo that is covered by a bill of lading, which is a contract between a shipper and a carrier. Cargo manifests are provided electronically to CBP 24 hours prior to lading by the carriers and non-vessel operating common carriers (NVOCC).

- Bill of Lading Number
- Foreign Port before vessel departs for United States
- Standard Carrier Alpha Code
- Carrier Assigned Voyage Number
- Date of Arrival at First U.S. Port
- U.S. Port of Unlading
- Quantity
- Unit of measure of Quantity
- First Foreign Place of Receipt
- Commodity Description (description/HTS–6)
- Commodity Weight
- Shipper Name
- Shipper Address
- Consignee Name
- Consignee Address
- Vessel Name
- Vessel Country
- Vessel Number
- Foreign Port of Lading
- Hazmat Code
- Container numbers
- Seal Numbers
- Date of departure from Foreign Port
- Time of Departure from Foreign Port

2. CBP also receives entry and entry summary data provided electronically by customs brokers or self-filing importers. This data is not required by law until *after cargo arrival* in the US. This data contains details about *importations.* An importation is merchandise that is being entered into the commerce of the United States

by an importer of record on behalf of an ultimate consignee. The importer of record is the party responsible for payment of any duties and fees. In most cases, the importer of record and ultimate consignee are the same party.

- Entry Number & Type
- Entry—Dist & Entry—Port
- Filer Code
- Importer of Record
- Ultimate Consignee
- Surety Number
- Filing Date & Time
- Importing Carrier
- Vessel Name
- Country of Origin
- Exporting Country
- Exporting Date
- Foreign Port of Arrival
- Estimated Arrival Date
- Entry Value
- Harmonized Tariff Schedule of the USA (HSUSA) (10)
- Manufacturer ID

Proposed New "10+2" Data

The Importer Security Filing and Additional Carrier Requirements NPRM published on January 2, 2008 generally would require 10 additional data elements from U.S. importers *prior to vessel loading* at foreign ports, and 2 data set items from carriers. The additional information would enhance CBP's ability to identify high-risk cargo shipments.

CBP's close partnership with the trade community is the key reason why the "10+2" NPRM was developed in a smooth and timely fashion. The trade's input during the consultative process as well as its participation in the Advance Trade Data Initiative (ATDI) has been instrumental in the successful crafting of the NPRM. Through the collaborative ATDI process, CBP was able to identify data that commonly exists, is currently used by the trade, and, if obtained in a timely fashion, would greatly benefit CBP's targeting and analysis of potentially high-risk cargo prior to U.S. arrival.

Additionally, CBP has been engaged with the Department's Advisory Committee on Commercial Operations, (COAC), which is comprised of government and industry representatives. In February 2007, COAC made almost 40 recommendations to CBP on how to implement the security filing or "10+2 initiative". CBP carefully studied and considered the COAC recommendations and agreed in full and/or in part to a majority of the recommendations.

1. Under the "10+2" NPRM, carriers would be required to submit a *vessel stow plan* and *container status messages* regarding certain events relating to containers loaded on vessels destined to the United States. The vessel stow plan is used to transmit information about the physical location of cargo loaded aboard a vessel. In general, if a container is listed on a vessel stow plan it is considered physically present on the vessel. CBP would receive the vessel stow plans *prior to U.S. arrival* and will compare the vessel stow plan to the containers listed on the manifest in an effort to identify unmanifested containers. Unmanifested containers are inherently dangerous since CBP has no way of performing risk analysis on the origins, contents, destination or actual intention of these rogue containers.

Container status messages are used within the shipping industry to report terminal container movements *(e.g.,* loading and discharging the vessel) and to report the change in status of containers *(e.g.,* empty or full).

2. Under the NPRM, 10 elements would be required for shipments other than those consisting entirely of foreign cargo remaining on board (FROB) and goods intended to be "transported" in-bond as an immediate exportation (IE) or transportation and exportation (T&E). The 10 required elements are:

- Manufacturer (or supplier) name and address
- Seller (or owner) name and address
- Buyer (or owner) name and address
- Ship to name and address

- Container stuffing location
- Consolidator (stuffer) name and address
- Importer of record number/foreign trade zone applicant identification number
- Consignee number(s)
- Country of origin
- Commodity Harmonized Tariff Schedule of the United States number

Under the NPRM regulations, five elements would be required for shipments consisting entirely of FROB and shipments consisting entirely of goods intended to be "transported" in-bond as an IE or IIE.

CBP is currently developing the process for complete integration of the "10+2" data elements into the ATS GUI. In addition OIOC and OFO are reviewing the data and creating new targeting rule concepts based on the SF elements that will be available. The data elements will be used to create new entity tables and allow link analysis capability to the end-user when fully developed. The new data elements will further refine the existing targeting platform and allow for further transparency in the overall maritime supply chain for national security targeting.

Question 4. When does the Customs and Border Protection plan to implement new "10+2" filing requirements to increase the amount of data it receives from shippers?

Answer. CBP's 'Importer Security Filing and Additional Carrier Requirements' or "10+2" NPRM was published in the *Federal Register* on January 2, 2008. The NPRM is available for public comment until March 18, 2008. At the conclusion of the comment period, CBP will carefully study and consider the comments it receives before drafting a final rule.

After the final rule is published in the *Federal Register,* a transitional or "interim" period will begin. During this interim period, CBP would give the trade ample opportunity to reconfigure their automated systems. The interim period is expected to last approximately 90 days. At the conclusion of the interim period, the final rule will go into effect and a 1-year "informed compliance" period would officially begin. During the informed compliance period, CBP would work closely with the trade to ensure that the required data is being filed correctly and that the impact on the trade is minimal in terms of data processing and data delivery.

It should be noted that the onus of the proposed "10+2" data requirements rests upon the importers and vessel carriers, and not the overseas shippers. The *importer or his agent* would be responsible for filing the complete, accurate, and timely importer elements of the Security Filing. For the purposes of the NPRM, importer means the party causing goods to arrive within the limits of a port in the United States.

Under the "10+2" NPRM, *carriers* would be required to submit a *vessel stow plan* and *container status messages* regarding certain events relating to containers loaded on vessels destined to the United States.

Question 5. Has DHS been approached with proposals from the private sector which would integrate maritime transportation data and content, business information, and open-source content? If so, what has the Department's reaction been to the concept?

Answer. CBP has attended and received presentations from the private sector regarding global data integration as part of our ongoing efforts to maintain and improve our cargo targeting strategy and systems. CBP fully supports and recognizes the efficacy of integrating a wide-range of open-source content and business information with maritime transportation data and will continue to explore our options with regards to both private sector and government-developed solutions.

Question 6. What is the status of DHS staffing plans that were required by the SAFE Port Act?

Answer. Sections 222 and 403 of the SAFE Port Act authorize additional positions for CBP. In FY 2008, Section 222 authorizes "not less" that 50 additional Supply Chain Security Specialists and Section 403 authorizes a "minimum" of 200 additional Customs and Border Protection officers (CBPOs). Observing Congressional direction, CBP has determined the locations to which the agency will deploy all the positions under the SAFE Port Act and has begun the process of hiring for these positions.

Question 7. What progress has your agency made in establishing a system to ensure that 100 percent of all incoming containers are scanned for radiation before being shipped to our shores?

Answer. The SAFE Port Act requires that three foreign ports pilot 100 percent scanning of U.S.-bound maritime containers using both radiation detection and imaging equipment. SFI fulfilled this mandate on October 12, 2007, when the ports

of Southampton, U.K., Qasim, Pakistan; and Cortes, Honduras became fully operational and now scan 100 percent of containerized cargo destined for the United States. In order to gather more data on 100 percent scanning in high-volume and transshipment ports, DHS and Energy (DOE) will also test, although in a more limited capacity, scanning systems in four additional ports: Hong Kong (now operationally testing); Busan, Korea; Salalah, Oman; and Singapore.

SFI sensor and image data gathered on containers bound for the United States are encrypted and transmitted in near real-time to CBP officers working in overseas ports and to the DHS National Targeting Center. This data is combined with other available risk assessment information to improve risk analysis, targeting and security of high-risk containers overseas. All alarms from the radiation detection equipment are resolved locally as is the current procedure under DOE's Megaports Initiative. For containers bound for the United States, SFI works with the host governments to establish protocols that ensure a swift resolution by the host government, which may include instructing carriers not to load the container until the risk is resolved, as per the interagency MOU on the "Interagency Nuclear and Radiological Technical Adjudication and Resolution Processes", signed on October 5, 2006.

Question 8. Standards for container locks and seals were required to be developed by the Department of Homeland Security by 2004. It is now 2007. The SAFE Port Act gave you additional time, but you have missed those deadlines as well. When will these standards be issued to reduce the risk of terrorists tampering with containers in transit?

Answer. On May 18, 2007, DHS notified ranking members of the U.S. Senate and U.S. House of Representatives of its decision not to initiate a rulemaking proceeding to establish minimum standards for securing containers in transit to the United States within the mandated timeline. DHS readily acknowledges that the process of securing the container is a critical component of a multi-layered strategy to secure the entire supply chain. However, the Department does not believe, at the present time, that the necessary technology exists for such a solution.

CBP has developed "Conveyance Security Device system and component technical requirements" which were published in a RFI on December 12, 2007.

DHS policy concerning applicability and use will be determined when an acceptable device(s) is approved.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO STEPHEN L. CALDWELL

Question 1. Why do you believe the Coast Guard will face challenges in expanding the exercise program in accordance with the SAFE Port Act?

Answer. The Coast Guard is currently involved in a variety of exercise programs that are designed to improve preparedness and response to a variety of security and maritime incidents. These exercise programs include the following:

- *Maritime Transportation Security Act (MTSA):* MTSA regulations require that the Coast Guard Captain of the Port and the area committee conduct or participate in exercises to test the effectiveness of area plans annually, with no more than 18 months between exercises. These exercises can test any portion of the area plans such as raising security levels, ensuring access control, or communicating threat information to the public.
- *Area Maritime Security Training and Exercise Program (AMStep):* The Coast Guard initiated the Area Maritime Security Training and Exercise Program in October 2005. This program was designed to involve the entire port community in the implementation and improvement of the Area Maritime Security Plan. This program supports the required MTSA exercises.
- *Port Security Training Exercise Program (PortSTEP):* The Coast Guard and TSA initiated the PortSTEP program in August 2005. PortSTEP is an exercise program designed to involve the entire port community, including public governmental agencies and private industry, and is intended to improve connectivity of various transportation modes and enhance area plans. Between August 2005 and October 2007, the Coast Guard expected to conduct PortSTEP exercises for 40 area committees and other port stakeholders.
- *Spill of National Significance (SONS):* The Coast Guard developed the SONS exercise program for response to oil and hazardous substance spills. This program focuses on exercising the entire National Response System at the local, regional and national levels for oil and hazardous material incidents that result from unintentional causes, such as maritime casualties and natural disasters. For example, the SONS exercise in June 2007 tested the response and recovery

to an oil and hazardous materials release in the wake of a large scale earthquake in the Mississippi and Ohio river valleys.

The SAFE Port Act included several new requirements related to security exercises, including the establishment of a Port Security Exercise Program to test and evaluate the capabilities of governments and port stakeholders to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism, natural disasters, and other emergencies at facilities that MTSA regulates. Additionally, the Act also required the establishment of a port security exercise improvement plan process that would identify, disseminate, and monitor the implementation of lessons learned and best practices from port security exercises. Given these existing programs, these new exercise requirements could be a challenge for the Coast Guard due to issues of scope, structure and participation, for example:

- *Scope:* The Coast Guard is currently conducting a variety of port security exercises with numerous different stakeholders (see exercise programs listed above). Given the similarities among these exercises it is unclear how the new program would differ or overlap from what is in place. The challenge for the Coast Guard will include setting the scope of the program to determine how the exercise requirements in the SAFE Port Act differ from area committee exercises that are currently performed. Also, in Coast Guard exercises conducted to date, recovery has not been substantially tested. In our past work, we found that Coast Guard terrorism exercises frequently focused on prevention and awareness, but often did not include recovery activities. With the SAFE Port Act requiring that exercises focus on preventing, preparing for, mitigating against, responding to, and recovering from acts of terrorism, natural disasters, and other emergencies, an expansion of the Coast Guard exercise program may be necessary to meet each of these new exercise requirements. Additionally, the Coast Guard currently has a process in place for gathering and disseminating lessons learned from exercises. While the SAFE Port Act requires a port security exercise improvement plan process that would identify, disseminate, and monitor the implementation of lessons learned, it is not clear how this would differ from the process the Coast Guard is currently using.
- *Structure:* Many of Coast Guard's security efforts and exercises have been focused on the area security plans in place at each port. While these plans are used to identify and reduce vulnerabilities to security threats throughout the port area, they do not focus on natural disasters. While the SAFE Port Act does not call for revising area plans to include all-hazard planning, it does contain a requirement that the Port Security Exercise Program test all hazards. On the basis of our prior work, we found there are challenges in using area committees and plans as the basis for broader all-hazards planning. The challenges for the Coast Guard includes determining the extent that security plans can serve all-hazards purposes as well as the ability to conduct natural disaster exercises when area security plans do not provide natural disaster guidance.
- *Participation:* According to the Coast Guard, as the primary sponsor of many of the exercise programs, it faces a continuing challenge in getting comprehensive participation in exercises. With the new exercise program requirements contained in the SAFE Port Act, the Coast Guard could be facing additional or expanded exercises. This may add to the exercise burden that port stakeholders already face, and the Coast Guard could continue to face the challenge of ensuring adequate participation.

Question 2. Your testimony states that your preliminary observations on the requirement of 100 percent scanning for all containers entering into the United States "potentially creates new challenges for CBP in terms of integrating this with existing programs, working with foreign governments, overcoming logistical barriers, testing new technology, and determining resource requirements and responsibilities, and other issues." Can you discuss these potential challenges in further detail?

Answer. While my oral comments provided limited information on challenges, our written statement contains more details. The following is a summary of challenges we have already identified:

- *CBP may face challenges in balancing the 100 percent scanning requirement with current international risk-based security practices and there is no assurance that it will provide a greater level of security than these practices.* CBP may have difficulty requiring 100 percent scanning while also maintaining a risk-based security approach that has been developed with many of its international partners. Currently, under the CSI program, CBP uses automated targeting tools to identify containers that pose a risk for terrorism for further inspection before being placed on vessels bound for the United States. As we have previously re-

ported, using risk management allows for reduction of risk against possible terrorist attack to the Nation given resources allocated and is an approach that has been accepted government-wide. According to CBP and foreign customs officials we spoke with, 100 percent scanning may actually provide a lower level of security than the current method of targeting and examination using risk-based methods. CBP officials stated that simply getting more scanning images does not necessarily imply that customs is doing a better job in providing more security. Similarly, international officials we spoke to stated that the risk management approach directs resources to where they are most needed, whereas scanning 100 percent of containers is inefficient because it directs too many resources in one activity—scanning—and diverts the focus away from those container shipments that pose the highest risk. According to these officials, under the current risk management system, customs officers tend to review the scanned images of high-risk containers in a very thorough and detailed manner. However, if the officers must review scanned images of all containers, the review may not be as thorough, as the officers could lose focus due to the sheer volume of work. If images are not properly or thoroughly analyzed, this could lead to a degradation of security.

- *The United States may not be able to reciprocate if other countries request 100 percent scanning and logistical feasibility and technological maturity are unknown.* The CSI program is based on a series of bilateral, reciprocal agreements with foreign governments that allow the foreign governments the opportunity to place their customs officials at U.S. seaports and request inspection of cargo containers departing from the United States and bound for their home country. According to CBP officials, the SFI pilot, as an extension of the CSI program, allows foreign officials to ask the United States to reciprocate and scan 100 percent of cargo containers bound for those countries. Although the Act establishing the 100 percent scanning requirement does not mention reciprocity, CBP officials have told us that the agency does not have the capacity to reciprocate should it be requested to do so, as other government officials have indicated they might when this provision of the 9/11 Act is in place. Just as the United States does not have the capacity to scan 100 percent of exports, logistical feasibility and technological maturity problems may make it difficult for foreign seaports to scan 100 percent of U.S.-bound cargo containers. For example, many ports may lack the space necessary to install additional equipment needed to comply with this requirement. Additionally, we observed that scanning equipment at some seaports is located several miles away from where cargo containers are stored, which may make it time consuming and costly to transport these containers for scanning. Similarly, some seaports are configured in such a way that there are no natural bottlenecks that would allow for equipment to be placed such that all outgoing containers can be scanned, and the potential to allow containers to slip by without scanning may be possible. Further, it may be difficult to scan transshipment cargo containers—containers at a seaport for a very short period of time—as well as container that remains on board a vessel as it passes through a foreign seaport. In addition to logistical issues, integrated scanning technologies utilized to test the feasibility of scanning 100 percent of U.S.-bound cargo containers are not yet operational at all seaports participating in the SFI pilot. Moreover, agency officials have stated that the amount of bandwidth necessary to transmit scanning equipment outputs to CBP officers for review exceeds what is currently feasible and that the electronic infrastructure necessary to transmit these outputs may be limited at some foreign seaports.
- *Resource responsibilities and ownership issues have not been determined.* The 9/11 Act does not specify who would pay for additional scanning equipment, personnel, computer systems, or infrastructure necessary to establish 100 percent scanning of U.S.-bound cargo containers at foreign seaports. However, foreign government officials we have spoken to expressed concerns regarding the cost of equipment. They also stated that the process for procuring scanning equipment may take years and can be difficult when trying to comply with changing U.S. requirements. These officials also expressed concern regarding the cost of additional personnel necessary to: (1) operate new scanning equipment; (2) view scanned images and transmit them to the United States; and (3) resolve false alarms. An official from one country with whom we met told us that, while his country does not scan 100 percent of exports, modernizing its customs service to focus more on exports required a 50 percent increase in personnel, and other countries trying to implement the 100 percent scanning requirement would likely have to increase the size of their customs administrations by at least as much. The 9/11 Act also does not specify who will be responsible for managing

the data collected through 100 percent scanning of U.S.-bound containers at foreign seaports. However, the SAFE Port Act specifies that scanning equipment outputs from SFI will be available for review by U.S. Government officials either at the foreign seaport or in the United States. It is not clear who would be responsible for collecting, maintaining, disseminating, viewing or analyzing scanning equipment outputs under the new requirement. Other questions to be resolved include ownership of data, how proprietary information would be treated, and how privacy concerns would be addressed.

Question 3. Given your experience with the GAO's Container Technology Assessment Report of 2006 and the CSI program, when do you anticipate the technological performance standards for radiation scanning and nonintrusive imaging equipment, required under the SAFE Port Act will be finalized both domestically and internationally?

Answer. In April 2005, we recommended that CBP establish minimum technical criteria for the capabilities of nonintrusive inspection equipment at CSI seaports. Similarly, in 2006, the SAFE Port Act required CBP to establish minimum technical capability criteria and standard operating procedures for the use of nonintrusive inspection equipment and nuclear and radiological detection systems in conjunction with CSI. While CBP has developed minimum technical standards for equipment used at domestic seaports, CBP officials stated that their agency faces challenges in implementing this requirement overseas due to sovereignty issues and the fact that the agency is not a standard setting organization for equipment. Given the agency's reluctance to set such standards, we cannot predict when it will do so.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DANIEL K. INOUYE TO ANTHONY COSCIA

Question. The SAFE Port Act required that all containers entering high volume ports must be scanned domestically for radiation before December 31, 2007. Where does the Port of New York and New Jersey stand in terms of meeting this deadline? What barriers would prevent you from meeting this deadline?

Answer. At the Port of New York and New Jersey, Customs and Border Protection (CBP) currently scans 98 percent of all import cargo for radiation. The remaining 2 percent which CBP deems to be low risk is intermodal rail cargo originating in just one of our container terminals. Therefore we are eagerly anticipating the results of the rail pilot project in the Port of Tacoma to help us devise a meaningful way to scan the remaining 2 percent of our import containers for radiation.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. FRANK R. LAUTENBERG TO ANTHONY COSCIA

Question 1. From an industry perspective, what is needed from the government in terms of planning for response and recovery after a security incident or other disruption in trade? Are current plans for resumption of trade adequate?

Answer. The Strategy to Enhance International Supply Chain Security, which the Department of Homeland Security submitted to Congress earlier this year, provides a high level overview of national plans for response and recovery. However, these national plans need to be translated into port-specific plans in order to be effective. While some U.S. ports, including the Port of New York and New Jersey, have port recovery plans already in place, it is our understanding that the U.S. Coast Guard will be releasing guidance on and requirements for the development of port-specific recovery plans in the coming months. Existing plans will need to be updated to conform to the new guidance, which hopefully will include tactical information required for effective planning. Short of knowing what the Federal Governments plans and capabilities are for instance with regards to salvage and redeployment of personnel, it is difficult for us to fully determine if the current plans are sufficient to support the resumption of trade. Once these port-specific recovery plans are written or updated, it is essential that they be tested and exercised on a large scale including the participation of headquarters staff from various DHS agencies and neighboring ports.

Question 2. A task force led by your agency has recommended that the Federal Government collect a per-container fee to be used for port security. I assume the only way to do this is to collect it at every port, so as to not give any individual port a competitive advantage. How do you envision this to work?

Answer. The Port Security Task Force (PSTF) understands that the proposed security fee must be administered and collected so as to not give an advantage to one

port over any other. As a result, the PSTF has advocated that before the fee is assessed, the Department of Homeland Security, in cooperation with the Department of the Treasury, should conduct a study to evaluate different methods for fee administration, formulation and disbursement, together with an evaluation of current maritime industry methods. Consideration should also be given to the reallocation of Federal fees that are already collected from the maritime industry, to be used to cover port security costs.

Question 3. I understand the lack of Federal personnel is a major problem at some ports. What is the consequence of this understaffing at the Port of New York and New Jersey?

In the Port of New York and New Jersey, both the Coast Guard and Customs and Border Protection are plagued with staffing shortages. CBP estimates that they need approximately 10 percent more staff to conduct their port security missions. These staff shortages result in the inspection of certain high-risk containers being delayed beyond the national goal of 72 hours. Although these high-risk containers are eventually inspected, they (and any other containers on the same Bill of Lading) are unable to be moved pending the inspection, resulting in additional costs to the shipper. Locally, the Coast Guard is currently operating at 1996 staffing levels for one of their mission areas despite a 139 percent increase in volume of activity. Left unaddressed, these staffing limitations will adversely impact the free flow of commerce, safety and security.