THE SAFE PORT ACT: A SIX-MONTH REVIEW

HEARING

BEFORE THE

SUBCOMMITTEE ON BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

APRIL 26, 2007

Serial No. 110–31

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

48–906 PDF WASHINGTON : 2009

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

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM

LORETTA SANCHEZ, California, *Chairwoman*

JANE HARMAN, California
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
AL GREEN, Texas
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

MARK E. SOUDER, Indiana
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PETER T. KING, New York *(Ex Officio)*

ALISON ROSSO, *Director*
DENISE KREPP, *Counsel*
CARLA ZAMUDIO-DOLAN, *Clerk*
MANDY BOWERS, *Minority Senior Professional Staff Member*

CONTENTS

THE SAFE PORT ACT: A SIX-MONTH REVIEW

Thursday, April 26, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON BORDER, MARITIME,
AND GLOBAL COUNTERTERRORISM,
Washington, DC.

The subcommittee met, pursuant to call, at 1:14 p.m., in Room 1539, Longworth House Office Building, Hon. Loretta Sanchez [chairwoman of the subcommittee] presiding.

Present: Representatives Sanchez, Jackson Lee, Green, Souder, and Bilirakis.

Ms. SANCHEZ. [Presiding.] Good afternoon, and thank you all for being here today. I thank the members of the committee who are here.

I know that votes have just finished for the day, so some of our members who believed they would be here obviously are trying to beat the crowd at the airport and come to their home districts. We understand that.

The Subcommittee on Border, Maritime, and Global Counterterrorism will come to order.

The committee is meeting today to receive testimony on "The SAFE Port Act: A Six-Month Review."

I would ask the indulgence of my colleagues before we begin if we might take a moment of silence in honor of Congresswoman Juanita Millender-McDonald. For those of you who know anything about the entire process of the SAFE Port Act, Juanita's bill was what we used as the base for that bill. So I think it would be appropriate to take a moment of silence as we go into the weekend. We will have her memorial services on Sunday and Monday, and I know many of my colleagues will be back there for that.

So if we could take a moment of silence.

Thank you.

So first of all, let me thank all of the witnesses for joining us today and for your testimony on how the implementation of the SAFE Port Act is going.

As you know, the SAFE Port Act mandated many long-overdue improvements and advancements that will enhance our nation's port security once they are all implemented, but it is always about how you can have a great plan, a great study, but you need to implement it. So that is what we are here about today.

These issues are very complex. It requires a lot of agencies at different levels working together to make sure we get it all done. So today's hearing will have two panels.

The first will consist of government witnesses. I am very pleased that representatives from the Coast Guard, Customs and Border Protection, and the Transportation Security Administration are here to provide detailed information regarding how their agencies' implementation of the SAFE Port Act is coming along. In addition, I am looking forward to the Government Accountability Office's insight into the government's ongoing port security issues.

During the second panel, we will hear from a variety of port security stakeholders. I am very proud to represent an area where we have the ports of Los Angeles and Long Beach so close, and some of the committee members have been able to visit those ports. So I am really proud to have the Port of Los Angeles represented here today, and Tampa represented at today's hearing, as well as the International Longshore and Warehouse Union and the Marine Exchange of Southern California.

What I am looking for from this hearing is, 6 months later—I know it is early, but you have to realize that I was just having lunch today with an accountant, and if anybody knows anything of my background, you will know that I come from finance. And so, having the plan and implementing the plan and checking it every so often I believe is the only way we really get to whatever our desired goal is. That is why I am so happy that we are having this.

There are specific issues that I would like to hear about—Custom and Border Protection's progress on the planning and implementation of the year-long pilot project for C–TPAT third-party validation; the Coast Guard's current long-range vessel tracking capabilities; the TSA's and Coast Guard's progress in rolling out the TWIC, or the transportation worker identification card; and Custom and Border Protection plans for the 1-year pilot program to assess the risk posed by the empty containers at our ports.

Those are just a few of the issues. If you have any others that are burning that you think I need to worry about at night, then please talk about those also.

So I am looking forward to having some good dialogue about all these important issues under the SAFE Port Act, and I thank you for being here.

I now believe it is time for my ranking member to give his opening statement. So the gentleman of Indiana, I will give his time for the opening statement.

Mr. SOUDER. Thank you.

I want to thank all the witnesses, both on our first panel as well as the port directors and the representatives from the workers at the different port authorities for being here.

Approximately 95 percent of our overseas commerce travels by ship through the U.S. seaports. More than 12 million containers entered the United States last year, and that number grows annually. Port activities contribute more than $700 billion annually to our GDP.

The ability to protect this system from terrorist attacks and rapidly recover are essential capabilities for securing our homeland and maintaining our economic health.

The SAFE Port Act built upon the significant investments made by the departments, specifically by CBP and the Coast Guard, in securing our port infrastructure and global supply chains after

9/11. The public law strengthens exiting programs and creates new initiatives to develop a robust, risk-based system for securing the entire maritime transportation system from the point of origin through the supply chain, for safe and secure delivery into the United States ports.

I applaud the leadership of Mr. Lungren, Ms. Harman, Chairwoman Sanchez, as well as Ranking Member King and Chairman Thompson, for developing this legislation, as well as our late colleague, and moving it through the committee last Congress and onto the president's desk.

I look forward to hearing more from the witnesses about current port security efforts and the implementation of the new mandates. In particular, I am interested in an update on the transportation worker identification credential, minimum standards for securing containers, supply chain security programs, the secure freight initiative, and what is being done to enhance our ability to target high-risk containers.

The SAFE Port Act has been a truly bipartisan effort from the start to the finish in both bodies of Congress. The SAFE Port Act passed the House of Representatives on May 4, 2006, by a vote of 421 to 2, and the Senate on September 14, 2006, by a vote of 98 to 0. The legislation was signed into law on October 13, 2006.

To bring a bill through the process involving more than six committees, all the while in the midst of preparing for an election, shows the importance this body places on securing our ports and supply chains. You can be sure that there will be significant oversight, as well as congressional support, for the implementation of the 90-plus mandates in the law.

Thank you again, Madam Chair, for holding this hearing. I hope that the SAFE Port Act process will be a model that the committee will follow as we move to consider other pieces of legislation in the 110th Congress.

I would now like to yield the balance of my time to my colleague from Florida, Congressman Bilirakis, to welcome and introduce a fellow Floridian who will be presenting his testimony on the second panel.

Mr. BILIRAKIS. Thank you, Ranking Member Souder. I want to commend you and Chairwoman Sanchez for holding this hearing to examine port security and review of the SAFE Port Act.

I am pleased to welcome to our committee Mr. Richard Wainio, the director of the Port of Tampa, which is Florida's largest port and, although I am surely biased, one of our best, the best.

I recently spent a day at the port and learned about the good work being done there and the security challenges the ports across my state and around the country are facing.

I look forward to hearing your testimony today, sir, and thank the Madam Chairwoman and Ranking Member Souder. I appreciate it, and yield back the balance of my time. Thank you.

Ms. SANCHEZ. Thank you to both of you.

The chair will let other members of the subcommittee know that, under the committee rules, opening statements may be submitted from them for the record.

And now I welcome our first panel of witnesses.

Our first witness, Admiral Craig E. Bone, is the assistant commandant for prevention in the Coast Guard. In this capacity, he directs national and international policy and programs for port, vessel and facility safety and security, waterways management, including navigation systems, ice-breaking, bridge administration, and marine transportation system policy.

Does that mean you are helping the Canadians break those people out of the ice up there?

Admiral BONE. Yes, ma'am.

Ms. SANCHEZ. Admiral Bone is a 1977 graduate of the U.S. Coast Guard Academy. He began his Coast Guard career as a deck watch officer aboard the Coast Guard Cutter Hamilton in Boston, Massachusetts. His previous flag assignments include director of port security and director of the Inspection and Compliance Directorate.

Our second witness, Mr. Jayson Ahern, is the assistant commissioner, Office of Field Operations, Customs and Border Protection. As such, he oversees national programs and operations at 20 field operations offices, 326 ports of entry, 50 operational container security initiative ports worldwide, and 15 pre-clearance stations in Canada, Ireland and the Caribbean.

Whenever you need to get a hold of him, you can. I have experienced that.

Assistant Commissioner Ahern began his career with the U.S. Customs Service in San Ysidro, California. He has previously been assigned as the director of field operations in Southern California, and he was also the principal field manager of customs port operations in Los Angeles, California, and Miami, Florida. Assistant Commissioner Ahern is a graduate of Northeastern University.

Welcome.

Our third witness, Ms. Maurine Fanguy, is the program director of the transportation worker identification credential program, or TWIC—we have a lot of questions for you—over at TSA. She is a graduate of Virginia Polytechnic Institute and State University in Blacksburg, Virginia. She has worked for TSA for 1 year.

Prior to joining TSA, Ms. Fanguy provided business and technology consulting services to private and public sector clients at Accenture. She also worked on a wide range of homeland security-related projects, including border management issues and application of biometric technology as well.

Our last witness on the first panel is Mr. Stephen L. Caldwell, director, homeland security and justice issues, Government Accountability Office. In this capacity, he provides direct support to congressional committees and individual members of the House and Senate on maritime security and U.S. Coast Guard issues. In the aftermath of Hurricane Katrina, for example, he was detailed from GAO to the House Select Committee on Hurricane Katrina to help investigate the preparations for and the response to that disaster.

Mr. Caldwell holds a bachelor's and a master's degree from one of those great universities of California at Berkeley.

Welcome.

So, without objection, your written testimony will be put into the record. I will now ask each of you please to summarize your state-

ments or tell us whatever it is that you want to tell us for 5 minutes apiece, beginning with the admiral.

STATEMENT OF ADMIRAL CRAIG E. BONE, ASSISTANT COMMANDANT FOR PREVENTION, U.S. COAST GUARD

Admiral BONE. Good morning, Chairwoman Sanchez, Ranking Member Souder, and distinguished members of the subcommittee. I am Rear Admiral Craig Bone, U.S. Coast Guard, assistant commandant for prevention. It is a pleasure to appear before you today to discuss the Coast Guard's efforts in implementing the SAFE Port Act requirements.

The primary objective of the SAFE Port Act is stated as, "to improve maritime and cargo security through enhanced layered defenses." The Coast Guard decided that, as one of the primary organizations with specific responsibilities in implementing this objective, several facets within our organization have been intimately involved in achieving the requirements since the enactment on October 13, 2006.

I will address only a few of the SAFE Port Act requirements that the Coast Guard is responsible for, in the interest of time. Section 101, the development of salvage response plans within each area maritime security plan has been integrated into the 5-year plan update cycle established by the Maritime Transportation Security Act, or MTSA, of 2002. The area maritime security plan updates 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 of 2009.

Resumption of commerce and recovery of the marine transportation system following a significant disruption is an issue of national concern. The Coast Guard is currently developing a concept of operations and specific planning requirements and organizational structures with our other DHS partners, to ensure a focus on MTS recovery following a significant incident that disrupts the marine transportation system.

Progress within section 104 of the SAFE Port Act included a number of statutory requirements governing the implementation of the transportation worker identification credentialing program. The Coast Guard and TSA met the first timeline with posting of the TWIC final rule on January 1, 2007. We have also met several of the regulatory requirements established in the Act. For example, the TWIC rule, together with the merchant mariner credential supplemental notice of proposed rulemaking published on January 25, 2007, incorporated the provisions set forth in the Act for concurrent processing of TWICs and merchant mariner documents.

In section 107, the Act requires the secretary of the Department of Homeland Security to establish a long-range identification tracking system that the chairwoman had spoken about. This SAFE Port Act requirement demands a multifaceted approach, using the full range of classified and unclassified vessel tracking information, including some information purchased from vendors where appropriate.

The Coast Guard currently meets the tracking requirements of the Act. Currently, sufficient tracking information exists, but work is needed in the processing, the display, and training in the use of

this information. The long-range identification tracking notice of proposed rulemaking is still being developed and therefore did not meet the April 1, 2007 deadline.

The department is also working to establish a system through IMO that will provide an unclassified global tracking capability by the end of the year 2008, as a part of an existing IMO convention, and make available to the United States a system that is compatible and interoperable with the global maritime community.

In section 109, the Coast Guard is supporting FEMA's National Preparedness Directorate's National Integration Center through training and exercise integration in implementing the requirements of this Act with regard to port security training.

We have made great progress. We have worked with MARAD in establishment of model courses. These courses are competency-based as required by the Transportation Security Act. In addition, FEMA and the National Preparedness Directorate has awarded a $6.18 million cooperative grant to Florida State University to develop courses meeting MTSA requirements and covering the eight core security-related topics under the SAFE Port Act.

Total port security grant funding available in fiscal year 2007 is $201,670,000. Those funds will be awarded based on analysis of risk and effectiveness of return on investment that the port entities have identified and applicants have identified. The initial reviews have been completed and actually final reviews are ongoing. It is anticipated the awards will be announced in May of 2007.

In accordance with the Act, the Coast Guard has also increased its foreign port assessments and we anticipate that all initial assessments of the 145 foreign ports that are trading partners with the U.S. will be completed by March, 2008, following which we will have examinations completed within every 2 years.

In conclusion, the Coast Guard is committed to working with the Department of Homeland Security team implementing all of the various statutes given within the SAFE Port Act. We continue to make headway on all fronts, and look forward to future progress and partnerships with the international, the federal, state and local port organizations, as well as the marine industry.

Thank you, Chairwoman, for the opportunity to testify today. I will be happy to answer any questions.

[The statement of Admiral Bone, Mr. Ahern, and Ms. Fanguy follows:]

PREPARED STATEMENTS OF JAYSON P. AHERN, ADM GRAIG BONE, AND MAURINE FANGUY

Introduction

The Department of Homeland Security appreciates this opportunity to discuss with you today the Security and Accountability For Every Port Act and the efforts of its components six months after its passage.

It is noteworthy that DHS, CBP, TSA, and the Coast Guard 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 Department of Homeland Security undertook immediately after 9/11 and has been implementing successfully ever since.

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

Area Maritime Security Plans.

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 (ACT) of 2002. The AMSP update will be performed by Federal Maritime Security Coordinators (FMSC) in consultation with their respective Area Maritime Security Committees (AMSC) 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 and researched with Federal Government partners. Consultation with national-level salvage industry representatives is continuing with the development and establishment of a Memorandum of Understanding (MOU) between the Coast Guard and the American Salvage Association of America. The MOU will establish a working partnership with goals of strengthening the communication and working relationship between the Coast Guard and the marine salvage and fire fighting industry to improve vessel and personnel safety within the industry, enhance national security preparedness and response, promote timely and professional salvage response to marine casualties, and enhance the protection of the environment along the nation's waterways.

Resumption of commerce and recovery of the marine transportation system (MTS) following a significant disruption is an issue of concern nationwide. 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 1st and 2nd, 2006. The symposium was attended by over 150 executive level participants from numerous branches of state and federal government, and 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 incident that disrupts the MTS. MTS recovery guidance will be harmonized with, and support implementation of, the forthcoming Strategy to Enhance International Supply Chain Security that is being prepared 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 will form the basis for revising Navigation Vessel Inspection Circular (NVIC) 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 (TSI), the Coast Guard is working to make AMSP coordination and procedures 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) and application of Incident Command System (ICS) principles and structures per the National Incident Management System (NIMS), is intended to support a consistent preparedness approach across all transportation disruptions without the need for additional port-level plans.

Maritime facility security plans.

The Department of Homeland Security 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. The Secretary can still waive the requirement after a determination based on a complete background check of the individual. These regulations 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 includes a complete background check, including a criminal history records check, a legal status check, and an intelligence and terrorist watch list check, thus satisfying 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.

Unannounced inspections of maritime facilities.

Currently, Coast Guard policy requires one annual inspection of each facility to be supplemented with periodic spot checks. The FY 2007 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, which will be filled during the 2007 transfer season, to add to the existing 350 facility inspectors. The Coast Guard has also created 61 reserve inspection billets to support additional inspections until permanent billets are filled this summer. This will ensure that each facility is inspected no less than two times per year, with at least one being an unannounced inspection. The Coast Guard conducted more than 7500 annual security inspections and unannounced spot checks of 3200 facilities in calendar year 2006, and will use the additional billets to increase these inspections. The 2006 inspections resulted in 465 violations which levied $1,892,000 in penalties.

Transportation Security Card.

The final rule for TWIC went into effect on March 26, 2007. With the passing of this critical milestone, this hearing provides an excellent opportunity to highlight program developments and describe how the Department of Homeland Security is incorporating lessons learned into an effective, efficient business plan for TWIC enrollment. This extremely important program is moving aggressively towards its objectives with a focus on making good security and business decisions. This leading edge program is developing essential processes, capabilities and expertise that will be beneficial to other programs.

The Department of Homeland Security has framed the program decisions and processes within the context of the nation's port security goals, including the need to:

- Identify authorized individuals who require unescorted access to secure areas of Maritime Transportation Security Act (MTSA) regulated facilities and vessels;
- Determine the eligibility of an individual for access through a security threat assessment;
- Ensure unauthorized individuals are denied access through biometric confirmation of the credential holder;
- Revoke access promptly for individuals who fail to maintain their eligibility;
- Apply privacy and security controls to protect TWIC information; and,
- Fund the program entirely by user-fees.

Achieving these ambitious goals has required creative planning, flexible implementation, effective stakeholder communication, and adaptive contract management. The basic program deployment philosophy has been a commitment to evaluate all practicable technical alternatives that will provide adequate port security and minimize adverse impacts, either economically or logistically, to United States citizens and the international trading system. This has been and will continue to be the program's implementation premise.

The Department of Homeland Security fully respects the fact that this program has significant operational implications to the economic wellbeing of the nation. Therefore, the Department is committed to ensuring that the program is tested, fully integrated and does not compromise security in any linked system TWIC is an advanced, sophisticated credentialing system that presents at least four groundbreaking technological challenges:

- TWIC uses the latest, most advanced federal government biometric and credentialing standards and for the first time applies them to the commercial sector.

- TWIC issues cards that work anywhere in the nation's private port environment, involving multiple potential companies and industries, by anyone working in a secure area.
- TWIC has not only unparalleled flexibility, it involves mass scale. There will be over 750,000 card holders working at 3,200 ports.
- TWIC security checks will be integrated into all of TSA's vetting programs creating potential security synergies throughout the entire transportation sector.

In other words, the hard part is not the card; the challenge is the network behind the card. The landmark technical principle underlying TWIC's ability to authenticate a person's identity includes three factors. When using the full extent of TWIC's authentication ability each person can be identified by:

- Something they know—a worker's Personal Identification Number (PIN);
- Something they have—the TWIC credential; and
- Something they are—a biometric.

With these considerations in mind, the below provides an overview of milestones completed, program plans, and how the Department has incorporated the lessons learned from this pioneering program.

TWIC Milestones to Date.

Obviously, new processes and technologies require systematic pilot studies. The prototype study was deployed to 26 locations in the areas of Los Angeles/Long Beach, Wilmington/Philadelphia and Florida's deepwater ports. The prototype TWIC was successfully issued to more than 4,000 volunteer workers including truck drivers, longshoremen, container terminal, railway, and airport personnel. A name-based threat assessment was completed on each individual. A criminal background check was conducted by the State of Florida for the deep-water port volunteers. These efforts were a success on multiple levels; it provided invaluable experience and a much deeper understanding of the technical and logistical challenges.

Security improvements cannot wait until TWIC is fully deployed. The Department has gone forward with significant interim security enhancements and actions during TWIC's initial development phase. These actions included:

- The Coast Guard worked effectively with the National Maritime Security Advisory Committee (NMSAC) to define secure areas. This definition will have a direct impact on over 10,000 vessels and more than 3,200 facilities. These secure areas delineate where a TWIC will be required for unescorted access.
- The joint rulemaking process between the Coast Guard and TSA was accelerated resulting in TWIC Notice of Proposed Rulemaking (NPRM) being published on May 22, 2006.
- The Coast Guard and TSA worked with industry partners to develop an interim process that compares a worker's biographical information against terrorist watch lists and immigration databases.
- Facility owners, facility operators and unions submitted worker names, date of birth, and, as appropriate, alien identification number. To date TSA has completed 750,000 name based threat assessments on port workers and longshoreman. This task will be repeated this summer to keep the assessment fresh. These assessments are interim measures and do not include the criminal history records check or biometric credential that is part of TWIC.

TWIC Rule and Stakeholder Input.

The TWIC rule was posted on the TSA and Coast Guard websites on January 1, 2007, and published in the Federal Register on January 25, 2007. The rule is the result of extensive public involvement and interagency coordination. In addition to the direct involvement of the National Maritime Security Advisory Committee, TSA and the Coast Guard held four public meetings in Newark, NJ, Tampa, FL, St. Louis, MO and Long Beach, CA. Over 1,900 comments were received from workers, port owners and operators, small businesses and others affected by the new program. All comments were carefully considered and significant changes were made to the NPRM in the development of the Final Rule. These changes include:

- The Coast Guard and TSA delayed the requirement to purchase and install electronic readers to allow for additional field testing, technology improvements, and more public comment.
- An expedited interim threat assessment process was created for new hires so that they may go to work pending completion of the full threat assessment.
- Immigration requirements were expanded to permit certain Visa-holders who are prevalent in the maritime industry to apply for a TWIC.

The rule also meets SAFE Port Act requirements to concurrently process TWICs and merchant mariner's documents, and to include a provision to enable newly hired workers to begin working after TSA conducts an initial threat assessment. In addi-

tion, the TWIC NPRM and Final Rule include provisions that respond to comments received from workers subject to similar threat assessment programs. These include:

- Creating a new process where TSA can make a determination that a security threat assessment conducted by another government agency is comparable, eliminating redundancy and reducing costs for workers;
- Providing workers more time to apply for an appeal or waiver;
- Streamlining the process, jointly with the Coast Guard, for merchant mariner credentialing and ensuring that there was no duplication of requirements resulting from the TWIC process.

TWIC cards will be required not only for port facility workers, but for anyone who seeks unescorted access to secure areas of a MTSA regulated facility or vessel, regardless of frequency. The workers covered by this rule include certain truck drivers, rail employees, security guards, longshoremen, as well as all U.S. merchant mariners. TSA will use the time tested security assessment procedures and standards that are currently used for commercial motor vehicle drivers licensed to transport hazardous materials, known as Hazardous Material Endorsements (HME). In short, TWIC will be issued to workers who successfully complete a security threat assessment, which includes: (1) a check against terrorist watch lists, (2) an immigration status check, and (3) a FBI fingerprint-based criminal history records check.

TWIC Card Readers.

The TWIC rule does not currently include a requirement for owners and operators to use card readers. This was done as a response to important public comments received on the NPRM and concerns from Congress expressed in the SAFE Port Act. The card reader requirement is being formulated and coordinated by extensive technical input from industry and the public. In the interim, workers seeking unescorted access to secure areas will present their cards to authorized personnel, who will compare the photo, inspect security features on the card, and evaluate the card for signs of tampering. At facilities with various sophisticated access control systems, the magnetic stripe on the credential could be used to grant or deny access at entry gates. The Coast Guard will also institute periodic unannounced checks to confirm the identity of the holder of the TWIC.

The Department of Homeland Security will continue to work closely with all interested parties to address the ever evolving technology issues. The TWIC technical architecture is compatible with Homeland Security Presidential Directive (HSPD) 12 and Federal Information Processing Standards (FIPS) 201-1 requirements which provide an open standard that will ensure interoperability and real-time exchange for supply chain security cooperation between the Department and the private sector. The applicant's photograph, name, TWIC expiration date, and a unique credential number are printed on the card. An integrated circuit chip on the card stores two fingerprint minutia templates and a PIN as well as a digital photo of the applicant, the applicant's name, and card expiration. The embedded computer chip is capable of being read by both contact and contactless card readers and also contains the magnetic strip and linear bar codes.

In addition to previously conducted prototype testing, pilot test planning and discussions with interested port, facility, and vessel operators began late last year. The pilots will test access control technologies in real world marine environments. The National Maritime Security Advisory Committee is providing invaluable input regarding operational requirements and has recommended specifications for contactless biometric smart cards and card readers. Public feedback is being collected and analyzed on the recommendations. As part of the outreach efforts for the TWIC program and the Department's Port Security Grant Program the Department has met with a number of maritime interests to invite their participation in the pilot tests. The Department's objective is to include pilot test participants that are representative of a variety of facility and vessel types and sizes 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.

The Department of Homeland Security is currently reviewing Port Security Grant applications relating to these pilot studies and will announce awards later this spring. While the grant process is proceeding, TSA and the Coast Guard are working with Department test and evaluation experts to develop a comprehensive plan that addresses the unique pilot test challenges. The evaluation of the pilot tests will greatly facilitate the Department's efforts to propose a TWIC reader requirement rule that effectively addresses security requirements, maintains the flow of commerce, and protects the personal information used to validate the TWIC holder's identity.

Rollout Contract.

A key operational piece of the rollout plan was the award of a competitively bid, indefinite delivery/indefinite quantity contract to Lockheed Martin Corporation. The TWIC enrollment and systems operations and maintenance contract will include a Quality Assurance Surveillance Plan (QASP) that establishes detailed metrics to be monitored through the life of the contract and will determine whether the contractor will receive any award fee for services performed.

Lockheed Martin will establish approximately 130 enrollment centers near the port facilities where applicants will provide biographic information and fingerprints. This information will be transferred to TSA so they may conduct a threat assessment involving checks of criminal history, immigration, and intelligence databases. Once a worker successfully completes the threat assessment process, the government will produce the credential and send it to the enrollment center, where the worker will retrieve it. TWIC enrollment will begin initially at select ports based on risk and other factors and will proceed throughout the nation over the next 18—24 months.

TWIC Card Costs.

As required by Congress, the costs of the program will be borne by TWIC applicants. Therefore, the Department is obligated to look for practicable ways of controlling costs, eliminating duplicative processes, providing timely decisions, and, most importantly, ensuring accuracy and fairness.

The fees for a TWIC will be slightly lower than was anticipated in the Final Rule. A TWIC will be $137.25 for a card that is valid for 5 years. Workers with current, comparable background checks (e.g., 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 $36, although the Department has solicited comment on raising that fee.

The Department of Homeland Security fully realizes that these costs are not an insignificant amount to some workers. However, the Department feels that the costs compare very favorably with equivalent HSPD–12 compliant card fees and in some instances may actually reduce the costs for some workers. For example, the Coast Guard is in the process of completing a companion rule which will consolidate existing mariner credentials and streamline the application process for mariners who have already applied for the TWIC. This will reduce the overall cost burden for these workers. Preparations are underway to reduce duplication by having TSA provide the Coast Guard with electronic copies of the applicant's fingerprints, proof of identification, proof of citizenship, photograph, and if applicable the individual's criminal record, FBI number and alien registration number. This will eliminate the need for TWIC holding mariners to visit a Coast Guard Regional Exam Center to apply for or renew their Merchant Mariner Credential unless an examination is required.

Rollout Communication Plan and Pre-Enrollment.

Effective public communication is fundamental to the Department rollout plan. The TWIC program office has used the lessons learned from the prototype phase to develop a multi-dimensioned outreach strategy for all of the enrollment phases. A toll-free help desk, Frequently Asked Questions, informational brochures, and a centralized e-mail address will provide up-front assistance and guidance for workers, owners, and operators. These services include program information, response to enrollment questions, pre-enrollment assistance, lost/stolen card reporting, credential replacement support, updates on an individual's case, and information on appeals and waivers. Applicants are encouraged, but not required, to "pre-enroll" and provide biographic information at the secure TWIC web site which should help reduce waiting time at the enrollment centers. An additional service that is provided during pre-enrollment is an opportunity for the applicant to schedule an appointment for appearing at the enrollment center.

Lockheed Martin is required by contract to develop a communication plan to ensure that applicants, operators, and relevant industry associations are educated and knowledgeable about the TWIC enrollment process. The communication plan will identify TSA goals and responsibilities, contractor goals and responsibilities, port facility and vessel responsibilities, target audiences, communications processes, and supporting communication tools. A key plan element was the establishment of the TWIC Stakeholders Communications Committee. The initial committee meeting was held last month with new meetings on a regularly occurring basis. These meetings will serve as a forum to ensure sustained two-way communication with stakeholders and directly provide the most current, accurate program information. Additionally, Lockheed Martin will facilitate rollout communications by deploying advance teams prior to the opening of enrollment centers to seek input and communication from local port officials, field federal agents, and local stakeholders.

Enrollment Centers.

Enrollment sites will be operated by trusted agents who are employees of a vendor under contract with TSA. These trained agents will have undergone a TSA security threat assessment before being allowed to collect data. The trusted agents will provide applicants with a privacy notice and consent form, by which the applicant agrees to provide personal information for the security threat assessment and credential. The trusted agents will verify an applicant's identity, confirm the accuracy of biographic information, collect biometric information (a full set of fingerprints and a facial photograph), and obtain the applicant's signature on the enrollment documents. The contract performance parameter for the trusted advisor enrollment process will be an average enrollment time of 15 minutes. The enrollment process for a pre-enrolled applicant is fully expected to take less time. Focused planning that fosters convenience for applicants will benefit workers as well as garner process efficiencies.

Data Security Vetting and Card Issuance.

After enrollment, an applicant's data is sent to the TSA system, and the vetting process (i.e., terrorism database, criminal history records check, immigration check) is started. One of the top technical challenges to introducing the new technology associated with TWIC is ensuring that the data is appropriately and efficiently transmitted to the appropriate destinations. The Department intends to enhance security synergies and efficiencies by using the same screening IT systems used for security screening in other programs. These efficiencies, however, require the Department to be absolutely certain that the stability or security of this larger vetting system is not jeopardized. Rigorous performance testing, and the accompanying scheduling complexities, is the only way to know for certain that satisfactory technical integration has been achieved.

Once the technical integration has occurred, it is anticipated that the TWIC threat assessment processing time will be similar to that experienced in the HME program. Since the inception of the HME program, threat assessments have frequently been completed in 3 days or less. During this same period the average time for completing HME threat assessments has been approximately 14 days, which includes all appeals and waivers. The process will be impacted by steps where there is minimum governmental control. For example, applicants need to promptly provide corrected records, and respond to initial determinations. Other anticipated factors that could result in processing delays include an applicant providing incorrect information, watch list determinations, evaluation of the nature of threats, whether the applicant is currently under criminal investigation, and confirming immigration status that is not available in electronic format. Nonetheless, the 14 day average for processing the HME assessments includes the time required to meet the same threat assessment challenges that will be faced with TWIC.

If TSA determines that an applicant does not pose a security threat, the applicant's information is sent for card production. After the card is developed it is sent to the enrollment center, where the worker will be notified to pick up the card. Due to the secure nature of the credential, the smart cards are shipped as "inactive." An applicant must verify his or her personal identity by providing a biometric (i.e., fingerprint) that is matched to the cards electronic template. After identity is verified, the applicant selects a secret PIN which is stored on the card as an additional identity authentication factor.

Worker Redress/Waivers/Appeals.

If an applicant is denied a TWIC they will be notified of the reason and instructed on how to apply for an appeal or waiver. All applicants have the opportunity to appeal a disqualification and may apply to TSA for a waiver. .

The standards for denial of a TWIC are the same standards that apply in the HME process. Any applicant who is subject to removal proceedings or an order of removal under the immigration laws of the United States is not eligible to apply for a TWIC. An individual will be disqualified if he or she lacks legal presence and/or authorization to work in the United States, has a connection to terrorist activity, or has been determined to lack mental capacity.

A person will also be denied a TWIC for a criminal history involving certain disqualifying crimes. TSA received valuable NPRM comments on the list of disqualifying crimes and decided to fine tune the list to better reflect crimes that are more likely to result in a terrorism security risk or a risk that the individual may engage in a transportation security incident. Permanent disqualifying criminal offenses include: espionage, sedition, treason, terrorism, improper transportation of a hazardous material, unlawful possession, use or sale of an explosive, murder, threats to a place of public use (government facility, public transportation system, or infrastructure facility), violations of the Racketeer Influenced and Corrupt Organizations

(RICO) Act in which the predicate act is one of the permanently disqualifying crimes, or a crime involving a transportation security incident. A transportation security incident is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

Individuals are ineligible for a TWIC if convicted in the last seven years or incarcerated within the last five years of the following crimes: Unlawful possession, use or sale of a firearm or other weapon, extortion, fraud, bribery, smuggling, immigration violations, distribution or importation of a controlled substance, arson, kidnapping or hostage taking, rape or aggravated sexual abuse, assault with intent to kill, robbery, RICO violations that do not involve a permanent disqualifying crime.

The appeal process involves ensuring that the information on which TSA bases its threat assessment is completely accurate. This process allows the applicant to correct the record on which that threat assessment occurs.

Fairness and accuracy in TWIC waiver determinations are further ensured by an opportunity for independent review by an Administrative Law Judge. As previously noted, the regulations provide a lengthened period for appealing denial of waivers, from 30 days to 60 days, to accommodate workers who tend to travel for extended periods of time. Furthermore, the regulations allow a worker to file a request for a time extension after the deadline has passed by filing a motion describing the reasons why they were unable to comply with the timeline. The extra procedural measures are intended to give workers every reasonable chance to bring legitimate concerns and issues to the attention of people who are trying to make the best and correct decision regarding security risks.

Lessons Learned and Future Efforts.

The initial rollout of TWIC will be focused on the maritime mode. However, once the initial maritime rollout is complete the Department of Homeland Security will evaluate deployment of this program in other modes of transportation. The analysis and planning for any resulting decision will benefit from the experience, technical expertise, and lessons learned that evolved under the TWIC program.

There are several vital lessons learned during the development of this program that must be prominently considered in future efforts:

- Look for *efficiencies in duplicative regulatory processes.* As noted previously, TSA and the Coast Guard are developing procedures for the sharing of mariner 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.
- *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. A Small Business Compliance Guide is also being produced and distributed to assist small businesses in their implementation of the program.
- *When practicable, preserve State regulatory flexibility.* Mariner regulations and port security plans preempt state regulations. However, TSA does not preempt States from requiring background checks and badging systems in addition to TWIC. States may need to set standards for important purposes other than terrorism threats.
- *Plan for privacy.* All data collected at an enrollment center will be deleted from the enrollment center work stations. 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 are created during 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 emergent needs that span local, international, public, and private interests. This requires continual reevaluation of the scope and methods of contracting. The recent Lockheed Martin contract award is a culmination of Department efforts to date. Due to the nature of this task, however, the Department will need to continue to look for and implement adaptive planning, metrics, and changes to ensure this effort stays on track.

• *Don't expect a "silver bullet' technology solution.* Evolving technology, such as card readers, creates 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.

• *Place the highest value in stakeholder input; it is time well spent.* The public hearings, comments to the NPRM, meetings with operators and associations, and contributions of advisory councils all added pure value. The Department came away from each and every one of these efforts better informed about the challenges, the unacceptable impacts, and the practicable options for protecting United States ports.

Long-range vessel tracking.

The Coast Guard currently meets the intent and tracking requirements of the Act using the full range of classified and unclassified vessel tracking information available. However, it takes up to two years to develop and finalize a regulation, and the Long Range Identification and Tracking (LRIT) NPRM is still being developed and, therefore, did not meet the April 1, 2007 deadline. The Act requires the Secretary of the Department of Homeland Security 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

• *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 information, 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, but work is needed in the processing, display, and training in the use of this information.

International:

The Departments work to establish a system through the International Maritime Organization (IMO) will provide an unclassified global tracking capability by the end of 2008 as a part of recently adopted amendments to an existing IMO convention and make available to the United States a system that is compatible and interoperable with the global maritime community. Since shortly after 9/11, the Coast Guard has been working with the IMO to implement a global tracking system for the types of vessels described in the Act. Following considerable U.S. 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 is more advantageous to the United States because it applies globally to all ships described in the Act rather than just those in U.S. waters or vessels intending to make port calls in the U.S. 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 that it is committed to support, and believes it will be able to implement capabilities to participate by the time the system comes into effect.

Interagency operational centers for port security.

Section 108 requires a budget and cost-sharing analysis for implementing interagency operations centers. The Department of Homeland Security did not meet the April 11, 2007 report deadline because it is are still working with agency partners to provide a consistent report. An interim letter has been sent, indicating that the report will be completed by July 30, 2007.

The establishment of interagency operations centers is currently not funded. In cooperation with Department of Justice (DOJ), Navy, and DHS Office of Science and Technology (S&T), three prototype centers have been established to date. The Coast Guard pilot projects for interagency operations centers are listed below. 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

* Sector Command Center

Additionally, a half dozen locations have been identified for short and medium term pilot projects to develop 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 constructs using collaboration tools.

When funded, the Command 21 project will field the capabilities necessary to create interagency operations centers as required by Section 108. This major establishment of proposed interagency operational centers for port security is a major system acquisition designed to close gaps in port and coastal maritime security.

Command 21 will:

- Improve maritime port and coastal security systems to complement the terrestrial Secure Border Initiative (SBI) Net;
- Improve unity of effort in a multi-agency operations center environment;
- Accelerate deployment of a net-centric tactical system that implements Department enterprise standards for the sharing of situation data and services across multiple Department interagency domains and Coast Guard systems; and
- Help address the security and safety issues posed by the 17 million smaller vessels that operate in port and coastal areas.

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:

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

Command 21 will close a critical gap between current capabilities and the desired interagency end state. Future interagency operations will 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 will publish tactical data in an open standard that allows other systems across multiple Department domains to subscribe to the information and use it according to the individual needs of each agency. It provides the maritime component of the Department of Homeland Security's Secure Border Initiative (SBI). Good government demands that both programs move forward in parallel to increase deterrence capabilities. If the two programs move ahead unevenly, illegal incursions will seek the path of least resistance. Moving ahead on both fronts will provide collaborative opportunities to leverage critical resources to broaden the impact of both programs toward securing the borders.

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) are being 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. Once the Coast Guard has completed evaluation of the proposed regulations and public comments, the final rule will be issued to implement the provisions of Section 109 as expeditiously as possible.

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.

The Coast Guard is engaged in discussions with Customs and Border Protection (CPB), Department of State, and Department of Labor to evaluate all options. In accordance with the Act, the Coast Guard will initiate a rulemaking to define identification documents necessary for foreign mariners calling on U.S. ports.

Risk assessment tool.

The Maritime Security Risk Analysis Model (MSRAM) is being used by Captains of the Ports/Federal Maritime Security Coordinators and Area Maritime Security Committees (AMSC) to analyze and prioritize scenario-based risks within their areas of responsibility and measure risk reduction potential in the evaluation of port security grant program proposals. AMSCs are required to validate the MSRAM on an annual basis. This was last completed in 2006 using MSRAM Version One, with an update expected to be complete in the summer of 2007 using MSRAM Version Two.

Port security grants.

The Coast Guard has been working with Department of Homeland Security 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, but the report is not yet complete. In the interim, a letter was sent to Congress stating that the April 11, 2007 deadline would not be met but that the Department expects to have the report to them by July 30, 2007.

The Port Security Grant Program (PSGP) provides grant funding to port areas for the protection of critical port infrastructure from terrorism. Fiscal Year 2007 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.

The total PSGP funding available in Fiscal Year (FY) 2007 is $201,670,000, and these funds were divided into four tiers of ports. Within Tier I, eight of the highest risk port regions have been identified and are eligible to apply for a fixed amount of funding based on risk. In many cases, multiple port areas have been grouped together to reflect geographic proximity, shared risk, and a common waterway. Port areas submitting applications within Tier II and III are eligible to compete for the FY07 PSGP but are not guaranteed funding. Section 112 of the Act also required that any entity addressed in an Area Maritime Security Plan also be eligible to apply. Tier IV has been 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 are eligible to compete with no guarantee of funding.

Funds will be awarded based on analysis of risk and the effectiveness of the applicants' proposed investments. Risk to port Infrastructure Protection Program Detail areas is assessed using a methodology consisting of threat, vulnerability, and consequence factors. The majority of port security grant funds—$120.6 million—will be available to eight Tier I ports or port areas considered 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 web site no later than 11:59 PM Eastern Standard Time on March 6, 2007.

The initial reviews were completed by the local Captain of the Port and results were forwarded to a national review panel comprised of representatives from the Coast Guard, the Transportation Security Administration (TSA), The Department of Homeland Security Infrastructure Protection (IP), Grants and Training (G&T), the Domestic Nuclear Detection Office (DNDO), and the Maritime Administration (MARAD) that convened for two weeks beginning April 9, 2007. It is anticipated that awards will be announced in the beginning of May 2007.

Port Security Training Program.

The Coast Guard is supporting the FEMA National Preparedness Directorate's National Integration Center, through Training and Exercises Integration (formerly a function of the Preparedness Directorate, Office of Grants and Training Division) in implementing the requirements of the Act relating to Port Security Training. Collectively, progress has been made in establishing the program delineated in the Act,

and there are a number of existing initiatives and new initiatives that taken together will address the requirements.

In response to Congressional mandate, the Coast Guard and MARAD prepared a Report to Congress and developed model courses for the training of facility and other personnel to meet the requirements in Section 109 of the Maritime Transportation Security Act of 2002. These model courses establish a competence-based standard and contain the majority 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 currently available via the MARAD 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 approval and certification process using the model courses as the guidelines for acceptance. The CG is currently revising the regulations for security training for facility personnel to ensure that all training is measured against a standard of competence, including the topics required under by 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 USCG are actively assisting DHS to ensure that this training will be consistent with existing standards and that it 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 to Federal, state and local personnel as well as to 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 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 coordinated by each State's governor-designated Training Point of Contact.

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. 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 2006, the Coast Guard has sponsored its own Area Maritime Security Training and Exercise Program (AMStep) that exercises the port stakeholder's ability to execute 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 calendar year 2006, these two programs collectively sponsored 53 port security exercises. 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. Exercise types have included basic and advanced table-top, 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.

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), and 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 change two to Coast Guard NVIC 09–02. These measures, outlined as objectives, are currently being revised by the Coast Guard Office of Incident Management Preparedness to align with the Department of Homeland Security Preparedness capa-

bilities-based planning model. All lessons learned and best practices are captured in the Coast Guard Contingency Preparedness System (CPS), which can be accessed by the entire Coast Guard. Additionally, through the use of Homeport, the Coast Guard's web-based communications and collaborations Information Technology application, Lessons Learned & Best Practices are made available to the entire port community (Federal, state, local, tribal and industry). Finally, the Coast Guard is working with the Department to offer and post select After Action Reports to the Department Lessons Learned Information Sharing (LLIS) system.

The implementation of the Coast Guard Remedial Action Management Program (RAMP) in May 2006 has assisted in the tracking and correction of numerous issues identified through current port security programs.

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.

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 the definition of "high risk facility" and the requirement for high risk facilities to conduct annual full-scale exercises.

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 nations ports of entry. That plan has been recently 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 973 RPMs at mail facilities, seaports, and land border crossings, and will deploy the first RPM in the air cargo environment this year. 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 98% of all containerized cargo at these 22 seaports. With the additional deployment of radiation screening equipment CBP currently scans 91% of the cargo and 81% of the passenger vehicles arriving from Canada; 96% of the cargo and 91% of the passenger vehicles arriving from Mexico, as well as 89% of arriving sea-borne cargo containers.

Since CBP began scanning cargo and conveyances for radiation, they have scanned over 151 million conveyances, and resolved over 840,000 alarms. This is a tremendous workload, and the SAFE Port Act authorizes 200 new CBP Officers in each of the next five 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 the New York Container Terminal (NYCT). Future deployments of ASPs will allow CBP to quickly differentiate between benign materials such as kitty litter or granite, while determining which shipments pose a true risk. This will perfectly fit with CBP's twin goals of increasing security while facilitating the flow of legitimate trade and people.

Inspection of car ferries entering from abroad.

CBP is currently developing a plan for the inspection of passengers and vehicles on ferries before the ferry embarks for the United States. Ferries reach the United States from four countries: Mexico, Canada, the Dominican Republic, and the British Virgin Islands. Currently, CBP is in the process of contacting the owners and operators of each ferry with a U.S. arrival to help determine the level of interest and the proper course of action. Once feedback from the owners and operators is received, CBP will reach out to the foreign governments of Mexico, Canada, the Dominican Republic, and the British Virgin Islands to further collaborate on implementing a plan.

Center of excellence for Maritime Domain Awareness.

The Coast Guard is assisting the Department of Homeland Security Science and Technology (S&T) Directorate to meet the requirements of the Act relating to a Center of Excellence for Maritime Domain Awareness (MDA). 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 MDA study as a central component of a broader system of research into maritime security. This solicitation is still open, and there has been a promising response from the academic community. 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.

Security of the International Supply Chain

The SAFE Port Act requires the Department of Homeland Security develop and implement a strategic plan to enhance the security of the international supply chain, including protocols for post-incident resumption of trade. A working group consisting of Department component subject matter experts was convened shortly after enactment and completed drafting the strategy in early February. The Department is currently consulting with appropriate groups including the Federal Interagency and Federal Advisory Committees and is on track to finalize the document and meet the July 10, 2007 submission deadline.

Automated Targeting System.

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 threat 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 with the Commercial Operations Advisory Committee (COAC), CBP has proposed 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 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.

CBP is currently developing a Notice of Proposed Rulemaking (NPRM) which will be published in the Federal Register along with a request for comments. 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 updates ATS. Since 2004, ATS has continually 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 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 resulted 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 (OCEN5) for maritime threshold targeting.

Container security standards and procedures.

The Department of Homeland Security 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. The Department does not believe that, at the present time, the necessary technology exists for such solutions. The Department is actively working with industry to test different technologies and methodologies that would provide economically and operationally viable enhancements to container security.

It should be noted that minimum security criteria for participants in the C–TPAT 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.

Container Security Initiative.

To meet their priority mission of preventing terrorists and terrorist weapons from entering the United States, CBP has partnered with other countries through their Container Security Initiative (CSI). CSI is another 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. Under CSI, which is the first program of its kind, CBP is partnering with foreign governments to identify and inspect high-risk cargo containers at foreign ports before they are shipped to United States seaports and pose a threat to the U. S. and to global trade.

The goal is for CBP's overseas CSI teams to conduct 100 percent manifest review before containers are loaded on vessels destined for the United States. However, in those locations where the tremendous volume of bills does not allow for the overseas CSI team to perform 100 percent review, CSI targeters at the National Targeting Center provide additional support to ensure that 100 percent review is accomplished. Utilizing the overseas CSI team and the CSI targeters at the National Targeting Center, CBP is able to achieve 100% manifest review for the CSI program.

Oversight of the CSI program is supported by automated tools for statistical analysis, an evaluation database to track and analyze any deficiencies identified during the evaluation process of the CSI ports, and a non-intrusive inspection (NII) equipment utilization database that tracks the use of NII equipment at CSI ports to include the downtime of the equipment.

Today, CSI is operational in 50 ports covering 82 percent of the maritime containerized cargo shipped to the United States. CBP is working towards strategically locating CSI in additional locations focusing on areas of the world where terrorists have a presence. CBP projects that by the end of 2007, CSI will be operational in 58 foreign seaports, covering over 85 percent of cargo destined for the United States. Declarations of Principles for each of the remaining 8 ports have been signed.

Customs-Trade Partnership Against Terrorism

The SAFE Port Act not only legislatively recognized the supply chain security industry partnership program known as 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 summer. 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. They have 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 four 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 has been made possible by adding Supply Chain Security Specialists (SCSS) 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 1,500. 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, with the identified additional staffing of 50 SCSS's being brought on board sometime in late calendar year 2008, C–TPAT would again see compliance with SAFE Port Act mandated timelines to be well within reach.

CBP has also developed a proposal through discussions with the COAC, where third parties will be used to validate supply chains where CBP currently lacks full access, and as a result, C–TPAT members are not receiving all the program benefits they are entitled to. Specifically, CBP will pilot using three to four accepted third party validators to perform reviews in China. A solicitation is currently posted to the Federal Business Opportunities website which outlines the requirements and conditions a firm wishing to be selected as a third party validator must meet. Those validation firms selected for this pilot must sign confidentiality agreements, maintain liability insurance, apply for SAFETY Act certification, and remain free from conflict of interests including having any direct or indirect control over the company which is being validated. The pilot program is voluntary, and as outlined in the Act, any C-TPAT member wishing to participate must pay for this service from the validating firm. Those validation firms selected will also be subject to background investigations. The solicitation closes on April 30th, and CBP anticipates that third party validations will begin in China in June.

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. In 2007, CBP will continue 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 SCSS's will conduct validations and begin revalidations of C–TPAT members' supply chains to ensure security protocols are reliable, accurate, and effective.

Pilot integrated scanning system.

Another example of extending port security outward is 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.

On December 7, 2006, the Department and the Department of Energy (DOE), in cooperation with the maritime industry and foreign government partners, announced Phase One of the SFI. The lessons learned and experience gained from Phase One represent critical steps in the process of determining whether the concept of 100% overseas scanning is technologically and economically feasible and the degree to which it increases the security of the international supply chain. Phase One will provide lessons and evidence on how this new, integrated suite of radiation detection and radiography technology can meld smoothly into the logistics, operations, and flow of commerce at each different port.

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 three additional foreign ports. This will provide a more complete analysis for SFI by including different operational and geographic settings at each port. The ports involved include: Port Qasim in Pakistan; Port Cortes in Honduras; Southampton in the United Kingdom; Port Salalah in Oman; Port of Singapore; and the Gamman Terminal at Port Busan in Korea.

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.

This initiative is the culmination of work with other Government agencies, foreign governments, the trade community, and vendors of leading edge technology. The scanning project is a first step toward realizing a greater vision of Secure Freight, a fully integrated global network for risk assessment.

The Department anticipates completing SFI on schedule, and reporting the results as per the requirements of the Act.

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.

Of particular note is the Coast Guard 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.

Foreign Port Assessments.

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

This two year cycle is consistent with the guidance contained in the FY–07 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 three year cycle. Additional resources (approx $6.7M which covered the costs of 32 new billets and associated operations and maintenance costs) were provided.

Office of Cargo Security Policy.

The SAFE Port Act established the Office of Cargo Security Policy within the Department of Homeland Security, and required that the Secretary appoint a Director to lead the office. This has been accomplished, with the Director of the Office of Cargo, Maritime, and Trade Policy being the designee.

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

The Department of Homeland Security and the Coast Guard have current and planned efforts to support the furtherance of maritime and cargo security. Fifty-seven percent of the Coast Guard Research, Development, Test, and Evaluation (RDT&E) fiscal year 2007 (FY07) project budget supports 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 (FY07 funding—$730K)	Maritime Biometrics, ID at Sea Boarding Team Connectivity Next Generation Underway Connectivity Boarding Officer Tools and Equipment Support
Compel Compliance (FY07 funding—$195K)	Anti-Personnel Stopping Mid-Sized Vessels

Mission Areas	Programs/Projects
Platforms and Sensors (FY07 funding—$915K)	Acoustic Buoy Multi-Sensor Performance Prediction Global Observer Small UAS Evaluations
Sector and Port Security Operations (FY07 funding—$389K)	Maritime Domain Awareness Community of Interest National Automatic Identification System
Miscellaneous (FY07 funding—$85K)	Net-Centricity Weapons of Mass Destruction

The Department of Homeland Security Office of Science and Technology (S&T) FY07 funds to the Coast Guard that support the furtherance of maritime and cargo security total $3,687K. The projects include:

Mission Areas	Programs/Projects
Boarding Team Support and Communications. (FY07 funding—$1050K)	Boarding Team Communications
Sensor, Data Fusion, & Decision Aids (Maritime) (FY07 funding—$2637K)	Visualization Tools Hawkeye Watch keeper Prototype Offshore Buoys for Vessel Detection Emergence Response Blue Force Tracking Swimmer/Diver Detection Global Observer

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. Through the S&T-established Capstone Integrated Product Teams (IPT), FY09–FY13 funding has been identified for the furtherance of maritime and cargo security through the Maritime Security Capstone IPT and the Cargo Capstone IPT.

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 September 2006. The establishment of this office will serve to strengthen CBP's ability to carry out their 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 enhanced. 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.

To meet the Congressional requirements of the SAFE Port Act, CBP is developing a resource optimization model (ROM) for the Office of International Trade. The objectives of the model are to: (1) optimally align the workforce to the Office of International Trade's performance outcomes and goals; (2) adequately staff the priority trade functions; and (3) comply with statutory requirements. The model will be designed to use the new office's performance objectives and goals as inputs to determine the right number and right mix of resources to facilitate legitimate trade.

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 work group will assess improvements to communications as a result of the reorganization, as well as some quantifiable measures for trade facilitation. Currently, the group is working together to find mutually beneficially process improvements to facilitate legitimate trade, which in turn will assist CBP in its trade enforcement efforts.

Domestic Nuclear Detection Office

The Department of Homeland Security greatly appreciated that Congress formally authorized the Domestic Nuclear Detection Office (DNDO) in the SAFE Port Act. Recently celebrating its second anniversary, DNDO is a vital component in the Departments ability to develop and implement WMD detection and response capabilities.

Conclusion

The steps the Department of Homeland Security is taking to implement the SAFE Port Act are and will be an extremely important aspect to the security of the nation's port facilities and vessels. Through the SAFE Port Act, Congress has recognized and bolstered many of our aggressive programs to protect our ports. We appreciate the close cooperative relationship the Department and its component agencies had with the House and Senate in the development of the Act, and look forward to the continued interaction to promote our mission and ensure the safety of American citizens and commerce.

Ms. SANCHEZ. Thank you, Admiral Bone.

We will go straight to Mr. Ahern for 5 minutes.

STATEMENT OF JAYSON AHERN, ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, CUSTOMS AND BORDER PATROL

Mr. AHERN. Good afternoon, Chairwoman Sanchez. It is very good to see you again, and Ranking Member Souder as well, and Congressman Bilirakis, Congressman Green. Thank you for the 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.

I would first like to thank the Congress for your continued interest and support on the important subject of maritime and supply chain security. In many ways, I look at the congressional passage of this legislation as an endorsement of CBP's approach to cargo security begun after the tragic events of September 11.

As you know, CBP has developed and implemented unprecedented initiatives to achieve our twin goals of both strengthening the security of containerized cargo entering our borders, all the while facilitating the flow of legitimate travel and trade.

CBP uses a multi-layered approach to ensure the integrity of the supply chain from the point of stuffing through arrival, as employed at our U.S. ports of entry. Through this approach, it includes trained CBP officers, a complement of technology automation and electronic information, as well as partnerships with trade organizations and many foreign governments throughout the world.

Madam Chairwoman, I know that you and a number of your colleagues, as you stated, have had the opportunity to see many of our operations at our ports in the United States, certainly Long Beach and Los Angeles are two critical ones that account for 44 percent of the container traffic coming into this country.

I know that Congressman Green had the opportunity to be a part of the congressional delegation that went down to the Port of Cortez to see our first phase-one of the Secure Freight Initiative, as well as many of the other members of this subcommittee, as well as the full committee under the chairman's leadership.

Certainly, I believe it is important to talk about many of the things you are already familiar with and some of the programs and the various components of the strategy we have had in place for a number of years. What I would like to do is highlight some of the critical things that we have done since the passage of the SAFE Port Act approximately 6 months ago.

Advance information: One of the key components of our strategy is making sure that we have sufficient advance information electronically received in advance of arrival. Certainly, the Trade Act and the 24-hour rule provide that information to us, but certainly today, working with the Departmental Advisory Committee on Commercial Operations, know as COAC, CBP is proposing a new security filing known as "10-plus-2."

It will provide additional information so that we can do more transparent security screening prior to lading overseas to make sure that we can continue to fulfill the requirements of the SAFE Port Act on electronic information. This will certainly help us.

C–TPAT: I know it has been a project of interest of this subcommittee in the past, and we look forward to talking about the third-party validators as we go forward. But certainly as we have evolved C–TPAT, we have steadily increased the rigor of the program and I would be happy to talk about that in some greater detail.

Today—just some numbers—there are 6,931 companies that have been certified into C–TPAT. Of those, 4,138 have been validated. CBP will meet the SAFE Port Act requirements and validate all members within 1 year of certification, and we will revalidate members not less than once every 4 years.

CBP has also had the discussion with the COAC, our Commercial Advisory Council, with the third parties on the validation process. This pilot program will be voluntary, as outlined in the Act, and any member wishing to have the payment of service for a validation can certainly begin with this process. I think it is important to note, too, that the solicitation that we have had out through the FedBizOpps actually closes on February 30 for those companies who want to be involved with the third-party validation pilot. I would be happy to talk in more detail.

RPM and NNI technology: Certainly, it is important for us to take a look to have the best technology deployed to our nation's ports of entry, including large-scale X-ray, gamma imaging systems, as well as a variety of radiation detection devices. It is important to note that the significant advancements made by CBP, as well as our departmental components, the Science and Technology Domestic Nuclear Detection Office, DNDO, has aided us in the rapid deployment of the technology to our ports of entry since the terrorist attacks of 2001. I want to talk to you a bit about some progress.

Certainly, before 9/11, we had no radiation portal monitors deployed at our ports of entry. Today, we have 966 RPMs at our seaports and land border ports. That accounts for 91 percent of all the trucks coming into this country across the northern border; 96 percent of all the trucks coming across the southern border of the United States; and 90 percent of the sea containers, close to 12 million sea containers coming into this country. About 90 percent of that universe is actually being scanned through radiation portal monitors and we will meet our objective of 98 percent by the end of this calendar year.

Just to put it in perspective, just 12 months ago in a maritime environment, when I reported to this subcommittee previously, we were only doing 37 percent of the sea containers. That is progress.

In addition to the strides in the area of radiation technology, we certainly continue to take a look at the latest advancements for non-intrusive inspection technology. This NII technology serves certainly as a force multiplier for us to detect anomalies, for not only just concealments of weapons with mass effect, but also narcotics. In fact, we scanned over five million scans last year using systems throughout fiscal year 2006.

Secure Freight Initiative: It is important for us to talk about that. It is building on the concept of our Container Security Initiative, with 50 ports covering, 82 percent of the worldwide global maritime container cargo destined for the United States has the opportunity to be scanned prior to be laded from the 50 ports. We will be at 58 by the end of this fiscal year. That will be for 85 percent of the containerized cargo coming into the country.

Importantly, and my final point, as I see I am close to time here, the Secure Freight Initiative. The secretary announced that on December 7. As stated, we had members of this subcommittee, as well as the full committee, in Honduras 2 weeks ago. We will be announcing the operational testing beginning in Pakistan in the next few days as well. And then the third location as required under the SAFE Port Act will be Southampton in the U.K., which will be operational towards the latter part of this summer or early fall. I would be happy to take more questions on that.

Thank you very much.

Ms. SANCHEZ. Thank you, Assistant Commissioner Ahern.

Ms. Fanguy, your turn. Am I saying that correctly?

Ms. FANGUY. You are saying it absolutely correctly.

Ms. SANCHEZ. Okay, go ahead.

STATEMENT OF MAURINE S. FANGUY, PROGRAM DIRECTOR, TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL PROGRAM, TRANSPORTATION SECURITY ADMINISTRATION

Ms. FANGUY. Good afternoon, Madam Chairwoman, Ranking Member Souder, and members of the subcommittee. My name is Maurine Fanguy, and I am the program director for the Transportation Worker Identification Credential Program, also known as TWIC. I am pleased to represent Assistant Secretary Kip Hawley here today.

Thank you for this opportunity to discuss TSA's progress on the TWIC program. Today, I would like to specifically focus on the technology and business processes that make TWIC successful.

To start off, I would like to answer one of the most frequently asked questions about TWIC: What makes a TWIC card different from the badges we all carry every day? There are four major differences between a TWIC card and one of these types of badges.

First, TWIC uses "smart card" and biometric technologies based on the most advanced federal government standards and, for the first time, applies then in the commercial sector. Second, TWIC issues cards that can be used at any port or vessel across the nation.

Third, TWIC has massive scale. Over 1 million cardholders will use the same credential across 3,200 facilities and on 10,000 vessels. In comparison with our prototype project, we will process in 1 day more credentials than we did in 1 year during the prototype.

Finally, TWIC issuance is based on very comprehensive security checks that involve data-sharing across multiple agencies. These checks are integrated into all of TSA's vetting programs, which means that we can connect the dots throughout the entire transportation sector.

In addition to the complexities of rolling out a sophisticated credentialing program nationwide, TSA and the Coast Guard established a regulatory framework for the program. The TWIC final rule, as Admiral Bone mentioned, was issued on January 1, 2007 and addressed over 1,900 comments from the public. The final rule includes important changes from the prototype, such as the ability to provide a discount for FAST-holders, mariners and HAZMAT truckers. The TWIC blueprint now aligns with the final rule.

TWIC is a sophisticated system powered by state-of-the-art technologies, and we are focused on a rigorous program to flight-test TWIC before we can go out to the ports. In other words, the hard part is not the actual card, it is the network behind the card. The TWIC network has five main components.

One, the pre-enrollment website allows workers to schedule appointments and provide biographic information ahead of time to make enrollment easier.

Two, the enrollment work station captures a worker's biometric and biographic information, and submits the information for security processing.

Three, the TWIC back end routes applicant information for processing, conducts data integrity checks, and manages the status of TWIC cards.

Four, the screening gateway is a TSA tool that aggregates security threat assessment data from the FBI, Citizen and Immigration Services, and watch lists. It is important to note that the screening gateway is used across all of TSA's vetting programs.

And five, the card production component electronically loads an applicant's information onto a TWIC smart card and then physically produces the card.

All the internal moving parts must work together to conduct accurate and timely security threat assessments. We recognize that TWIC will affect both businesses and port workers. That is why rigorous performance testing is the only way to ensure that TWIC is ready to go live. The program must not negatively impact commerce or people's livelihoods. Assistant Secretary Hawley has given us the mandate to get TWIC right the first time.

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.

We look forward to working with this subcommittee as we move forward with the TWIC program. Thank you for the opportunity to appear today, and I would be happy to answer any questions.

Ms. SANCHEZ. Thank you.

Mr. Caldwell, please, for 5 minutes or less.

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

Mr. CALDWELL. Thank you very much. I will take that as a challenge anyway.

Chairman SANCHEZ AND MR. Souder, I am very pleased to be here, and thank you for inviting me here.

I would like to tee off on a comment you made about, well, it has only been 6 months since the SAFE Port Act has been enacted. We have to remember that before the SAFE Port Act, there was MTSA and MTSA really laid a lot of the foundations here. I think it provided a very solid foundation in many ways.

The prior witnesses have already discussed a lot of the programs related to that, and they are also in my written statement, so I am not going to go into that in detail.

But I would like to add some important things about these efforts related to MTSA. First of all, they were brand new. Second, they were very ambitious. Third, they required very high levels of coordination across federal, state, local, private and international sectors. And third, the programs were being implemented by a brand new department. So we all had a lot of challenges there that I am sure my colleagues up here on the panel can affirm.

So it is not surprising that GAO's early work on a lot of these efforts found some basic management problems related to strategic planning, workforce planning, and coordination both within and across organizations. I can say that the more recent work that GAO has done has found that many of these programs are maturing. They are maturing at different rates, obviously, but some of the problems we are currently finding are more related to maintaining and improving current operations, as opposed to not having basic management foundations in place.

However, there are two ongoing concerns which we find in our work that is not only in our earlier work, but as well as the work here. The first concern is resources. Many of these programs have been challenged by a lack of resources, or at least the right resources. So many agencies have needed not only additional staff, but staff with the correct training and expertise.

Perhaps the Coast Guard is an example here, where there has not been a very large increase in the number of personnel, but there certainly has been a large increase in the number of responsibilities put upon the Coast Guard.

The second ongoing concern that our work has shown involves technology. While there has been a drive to use technologies for a wide variety of applications, not all of these technologies are as mature as we would like them to be, or at least as they need to be to get the job done. Also in some cases, even the newest technologies are not going to work if the right people are not using them. So even with the technology component, you still need people that know how to use it.

DOE's Megaport Program is an example of that, because we are providing the equipment to do radiation monitoring in foreign countries, but again we pretty much depend on those other countries once we leave to do all of the monitoring of the program, and

some of this equipment may need careful calibration and other things to make sure it is working appropriately.

Then along came the SAFE Port Act, and while it covered a very broad range of topics, everything from port issues to Internet gambling, much of it was aimed at strengthening the security regime that was put in place by MTSA. First of all, it formalized some existing programs into law. CSI and C–TPAT are good examples of these.

Second, it directed specific program improvements, for example, some of the recommendations made by either GAO, the IG, or congressional committees. And third, it set deadlines for specific actions to be accomplished. Some of these deadlines include actions for the implementation of TWIC, and 100 percent scanning for certain kinds of containers.

In many cases, Congress was approving existing programs, but it was clearly telling the agencies to do them better and to do them faster.

Getting back to resources, the congressional directives in the SAFE Port Act, whether it is to do something better or is to do something faster, all generally require additional resources. Additional resources certainly have been provided if you look at the budgets of these organizations.

But the question for Congress and the agencies is whether the increases in the budgets were commensurate with the additional responsibilities that they were given, and also some issues of whether they were allocated as well as they could have been.

Beyond security-related issues, when Congress created DHS there were clear concerns that DHS continue doing everything it was doing because all the component agencies came into DHS. In the case of the customs revenue function, Congress went as far as directing that specific numbers of people and positions be maintained in the customs revenue function, something that CBP has not done.

In the competition for resources within agencies, I think this is an example of the difficult choices that agencies are having to make when reallocating the resources between security and non-security priorities.

In terms of our work, we have made a number of recommendations involving the SAFE Port Act, as well as MTSA. We have worked with the agencies pretty closely in getting them to accept these recommendations, and they are certainly making attempts to implement those.

Looking ahead, we will continue to work with these agencies, as well as this committee and other representatives in Congress, to provide oversight, to keep our ports as safe as practical.

I would be happy to answer any questions. Thank you.

[The statement of Mr. Caldwell follows:]

PREPARED STATEMENT O STEPHEN L. CALDWELL

Madam Chairwoman and Members of the Subcommittee:

I am pleased to be here today to discuss port security and revenue functions related to provisions of the Security and Accountability for Every Port Act (SAFE Port

Act).[1] The nation's ports are the doorway 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 2004, for example, $423 billion worth of goods traveling to the United States arrived in 15.8 billion containers. Similarly, ports are vital for our energy supplies. In 2005, 55 percent of the nation's crude oil supply and natural gas supply was imported on seagoing tankers. The trade that passes through ports also generates substantial revenue for the U.S. government.

In our post September 11, 2001, environment, however, the potential security weaknesses presented by these economic doorways have become readily apparent. Ports present potential terrorist targets: they are sprawling, easily accessible by water and land, often close to urban areas, and contain facilities that represent opportunities for inflicting significant damage as well as causing economic mayhem. Further, they are conduits for weapons prepared elsewhere and concealed in cargo designed to move quickly to many locations beyond the ports themselves. At this time, the U.S. government does not require that all cargo destined for the United States be checked until it arrives.

Since the 9/11 attacks, a new port security framework has taken form. Much of this framework 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 through 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) establishment of a process to assess foreign ports, from which vessels depart on voyages to the United States. Much of this framework is administered by the Department of Homeland Security (DHS), itself a creation of the new security environment brought on by the September 11, 2001, attacks. This framework also attempts to balance security priorities with the need to facilitate legitimate trade.

One of the latest additions to this port security framework is the SAFE Port Act, which was passed and took effect in October of 2006. 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 any threats stemming from cargo containers; (2) established port security interagency operational centers at all high risk 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. The SAFE Port Act also mandated GAO to report to Congress on some topics related to maritime security, including (a) the security of ports overseas in the Caribbean Basin, (b) the background check program for transportation workers, including those seeking access to ports and other sensitive areas, and (c) the extent to which DHS continues to collect revenues at ports given the new emphasis on security.[3] This statement summarizes our work on these three mandates, though all of them have been, or will be, addressed in separate reports.

Over the past several years, we have examined and reported on many of the programs in this new homeland security framework. This statement is designed both to provide an overview of what we have learned about these programs and to describe, to the extent we have information available, what DHS is doing as a result of the SAFE Port Act requirements and the challenges it faces in doing so. This statement discusses more than a dozen programs and lines of effort, as shown in table 1.

---

[1] Pub. L. No. 109–347, 120 Stat. 1184 (2006).

[2] Pub. L. No. 107–295, 116 Stat. 2064 (2002).

[3] The SAFE Port Act had an additional requirement that GAO report on DHS pre-screening for charter and leased aircraft. Today's statement, with its primary emphasison maritime security and other activities at seaports, does not address this other reporting requirement.

Table 1: Summary of Programs and Lines of Effort Included 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.
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 officers visiting and assessing security conditions at foreign ports.
Port facility security	
Port facility security plans	Facilities are required to have security plans and security officers.
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 person who enter secure or restricted areas or transport hazardous cargo.
International supply chain—container security	
Automated Targeting System	Risk based decision system to determine cargo containers requiring inspection.
Container Security Initiative	Stationing CBP officers at foreign ports to help identify and inspect high risk cargo containers.
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.
Customs-Trade Partnership Against Terrorism	Partnership between private companies and CBP to improved international supply chain security.
Customs revenue functions	
Customs and Border Protection	Collect revenues applied to incoming cargo as appropriate based on tariffs and other laws and regulations.

Source: GAO.

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

- Programs related to overall port security, such as those for developing security plans, coordinating among stakeholders, and conducting exercises to test security procedures.
- Programs related more specifically to security at individual facilities, such as examining security measures and ensuring that only properly cleared individuals have access to port areas.
- Programs related more specifically to the international supply chain and to cargo container security, such as screening containers at ports both here and abroad.
- The extent to which DHS—and more specifically, CBP—has maintained the customs revenue function at ports formerly managed by Treasury.

This statement is based primarily on a body of work we have completed in response to congressional requests and mandates for analysis of maritime, port, and cargo security efforts of the federal government. The end of this report has a list of relevant GAO reports and testimonies. As such, the timeliness of the data that was the basis for our prior reporting varies depending on when our products were issued. In several cases, such as CBP's maintenance of effort on the customs revenue function, our findings are based on recent work specifically conducted in response to SAFE Port Act requirements. We conducted all of our work in accordance with generally accepted government auditing standards, and the scope and methodology for this work can be found in the respective products. Similarly, agency comments on the findings we cite can be found in the respective products. 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.

Summary

Regarding overall port security, the Coast Guard has generally implemented key requirements laid out in MTSA. It has established area maritime security committees, written area maritime security plans, conducted exercises to test such plans, and visited foreign ports to assess their compliance with international port security standards. In addition, the SAFE Port Act called for changes in several programs related to developing and testing security plans and coordinating information across agency lines. For example, it called for establishing interagency operational centers at all high-risk ports in the United States within 3 years. Three ports currently have such centers, which are designed to have a unified command structure that can act on a variety of incidents ranging from possible terrorist attacks to search and rescue and environmental response operations. Several new interagency operational centers are about to come on line, but in continuing the expansion, DHS may face such challenges as creating effective working relationships and dealing with potential coordination problems. Additionally, the SAFE Port Act required the establishment of a Port Security Exercise Program to test and evaluate the capabilities of various governmental and nongovernmental entities when faced with emergencies, and to improve the communication of lessons learned during the exercises. We have not specifically reviewed the implementation of these new requirements, but our past work suggests that the need to increase the already substantial exercise program, the need to quickly and thoroughly complete after action reports and the increased need for interagency coordination for the exercises may challenge port security stakeholders' efforts. The act also called for expanding a program in which the Coast Guard works with other countries to assess—and where needed, strengthen—their security procedures. The Coast Guard has developed plans for meeting these requirements, but it is likely to face challenges in developing sufficient staff to deal with the increased workload.

Regarding security at individual facilities at ports, MTSA has generally been implemented in that facilities have generally written and implemented security plans and the Coast Guard has inspected such facilities to verify compliance and take enforcement actions where necessary. However, the MTSA required transportation worker identification card has been plagued by delays. The SAFE Port Act called for such steps as mandating the frequency of Coast Guard inspections of facilities, requiring unannounced inspections, and directing the implementation of the initial phase of the transportation worker identification credential program by mid-2007. The Coast Guard, which is responsible for the facility inspection program, is likely to face challenges in putting enough trained inspectors in place, especially since many experienced inspectors are scheduled to rotate to other duties. The Transportation Security Administration (TSA), the agency responsible for implementing the identification credential, told us it has drawn up plans and schedules for implementing the program as required and has also brought on additional expertise to deal with past problems in the program's development. The effectiveness of these

steps is not likely to be known until the deadlines approach. While DHS has created the Screening Coordination Office to better coordinate the various 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 containers that move through ports, CBP has developed a layered security strategy to identify and inspect suspicious containers, and to work with both foreign governments and private firms to improve the security of the international supply chain. Many of the provisions in the SAFE Port Act dealing with container security served to codify existing programs in DHS—such as a program to place CBP officials in foreign ports to help target suspicious containers and a program where private companies agree to improve the security of their supply chains in exchange for reduced scrutiny over their shipments—it also expanded and provided additional guidance for those programs. The SAFE Port Act also required pilot programs to test new technologies or combine existing technologies for inspecting cargo containers. In our prior work on container security programs, we found that progress had been made, but challenges could affect ongoing efforts. Examples of progress made include increasing the number of foreign ports where U.S. officials are located and a rapid growth in the number of companies agreeing to take steps to secure their supply chains. Examples of challenges include ensuring adequate staff are available, and the inability to directly test the security measures used by different companies in their supply chains, particularly overseas.

Since DHS was formed, it has focused on homeland security issues, including striving to prevent terrorists entering or attacking the United States through its ports, but has not provided the same focus on ensuring the maintenance of customs revenue functions. Although it has improved recently, CBP has not maintained the mandated staffing levels for performing customs revenue functions, due in part to homeland security priorities. Despite a legislative mandate to at least maintain minimum specific numbers of staff in certain key customs revenue positions, the numbers of staff in several of these positions have declined since the formation of DHS. The numbers of staff in other positions that can help improve the performance of customs revenue functions have declined also. Further, CBP has not produced a strategic workforce plan to help ensure it has a sufficient number of staff with the necessary skills and competencies to effectively perform customs revenue functions. While CBP has made recent efforts to improve the management of its human capital for performing customs revenue functions, gaps in these efforts remain. Finally, CBP's public reporting on its performance of customs revenue functions does not ensure accountability. For example, despite being the second largest revenue generator for the U.S. government, CBP does publicly report on performance measures related to its customs revenue functions in its annual plans and Performance and Accountability Reports, the official documents agencies issue to Congress and the public to report program performance.

We have reviewed many of the MTSA and SAFE Port Act related programs and made 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 Challenges Remain

Port security in general has improved as a result of the development of organizations and programs such as Area Maritime Security Committees (area committees), 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, management of these programs will need to address additional requirements directed by the SAFE Port Act. Area committees and interagency operational centers have improved information sharing, but the types and ways information is shared varies. Area plans are limited to security incidents and 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 Committees and Interagency Operational Centers Have Become Important Forums for Cooperation and Information-Sharing across Agencies

Two main types of forums have developed as ways for agencies to cooperate and share information about port security—area committees and interagency operational centers. Area committees serve as a forum for port stakeholders, facilitating the dis-

semination of information through regularly scheduled meetings, issuance of electronic bulletins, and sharing key documents. MTSA provided the Coast Guard with the authority to create area committees—composed of federal, state, local, and industry members—that help to develop the area plan for the port. As of June 2006, the Coast Guard had organized 46 area committees. 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.

Interagency operational centers are currently located at three ports—Charleston, South Carolina; Norfolk, Virginia; and San Diego, California. These centers are designed to unite maritime intelligence and operational efforts of various federal and nonfederal participants.[4] Unlike area committees, they are operational in nature with a unified or joint command structure designed to receive information from multiple sources and act on it. However, the centers fulfill varying missions and operations, and thus share different types of information. For example, the Charleston center is led by the Department of Justice and focused solely on port security, while the San Diego center is led by the Coast Guard with missions expanding beyond port security to also include search and rescue activities, drug interdiction, and environmental response.

In past work, we have reported that these two types of forums have both been helpful in fostering cooperation and information-sharing.[5] We reported that area committees provided a structure to improve the timeliness, completeness, and usefulness of information sharing between federal and nonfederal stakeholders. These committees were an improvement over previous information-sharing efforts because they established a formal structure and new procedures for sharing information. In contrast to area committees, interagency operational centers can provide continuous information about maritime activities and involve various agencies directly in operational decisions using this information. While we have reported that interagency operational centers have improved information sharing, our past work has also shown the types of information and the way information is shared varies at the operational centers depending on their purpose and mission, leadership and organization, membership, technology, and resources.

The SAFE Port Act called for an expansion of interagency operational centers, directing the Secretary of DHS to establish such centers at all high-risk priority ports no later than 3 years after the Act's enactment. In addition to authorizing the appropriation of funds and requiring DHS to report on potential cost-sharing at the centers, it directs the new interagency operational centers to utilize the same compositional and operational characteristics of existing centers, such as the pilot project operational centers for port security. Currently two more centers are expected to be functional within weeks. These will be located in Jacksonville, Florida, and Seattle, Washington. Like the centers in San Diego and Norfolk, they will both be operated jointly by the Coast Guard and the Navy. In addition, the Coast Guard has developed its own operational centers, called sector command centers, as part of an effort to reorganize and improve its awareness of the maritime domain. These are being developed at 35 locations to monitor information and to support planned future operations, and some of these sector command centers may include other agencies on either a regular or an ad hoc basis.

Information sharing efforts, whether through area committees or interagency operational centers, face challenges in several areas. These challenges include:

- **Obtaining security clearances for port security stakeholders.** The lack of federal security clearances among port security stakeholders has been routinely cited as a barrier to information sharing, one of the primary goals of both

[4] Existing interagency operations centers are led by the Coast Guard or DOJ, and can include participation by representatives of organizations such as the Navy, U.S. Customs and Border Protection, Transportation Security Administration, U.S. Immigration and Customs Enforcement, other federal agencies, state and local law enforcement, or port security personnel. The Charleston center was created through an appropriation in the fiscal year 2003 Consolidated Appropriations Resolution (Pub. L. No. 108–7, 117 Stat. 11,53 (2003.)); the Norfolk and San Diego centers were established as (Joint Harbor Operations Centers" between the Coast Guard and Navy.

[5] 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).

the area committees and interagency operational centers. In previous reviews, we found that the inability to share classified information may limit the ability to deter, prevent, and respond to a potential terrorist attack. The Coast Guard has seen improvements based on its efforts to sponsor security clearances for members of area committees. 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 remains unclear.

• **Creating effective working relationships.** Another challenge associated with establishing interagency operational centers at all high risk ports is the difficulty associated with encouraging various federal, state and local agencies that have never worked together before to collaborate and share information effectively under new structures and procedures. While some of the existing operational centers found success with existing interagency relationships, other high-risk ports might face challenges establishing new working relationships among port stakeholders and implementing their own interagency operational centers.

• **Addressing potential overlapping responsibilities.** Overlapping leadership roles between the Coast Guard and FBI has been seen during port security exercises. While the SAFE Port Act designates the Coast Guard Captain of the Port as the incident commander in the event of a transportation security incident, the FBI also has leadership responsibilities in terrorist incidents.[6] It is important that actions across the various agencies are clear and coordinated.

• **Determining relationships among various centers.** The relationship between the interagency operations centers and the recently developed Coast Guard sector command centers is still to be determined. We have not studied either of these issues in depth, but they may bear watching.

Area Plans Are in Place but Do Not Address Natural Disasters

Area plans are another MTSA requirement, and the specific provisions of the plans 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 the plans.[7] Currently, 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. 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, the act specified that area plans include a salvage response provision identifying salvage equipment capable of restoring operational trade capacity. None of our past or current work specifically addresses the extent to which area plans now include this provision. We have, however, conducted other work that has a broader bearing on the scope of area plans, and thus potentially on this provision as well.

In a recent 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 do not include other issues that could have a major impact on a port's ability to support maritime commerce.[8] 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 faced by a port, both natural and man-made, 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 enhance the efficiency of port planning efforts because of the similarity in recovery plans for both natural and

---

[6] The Captain of the Port is a Coast Guard officer who enforce, within their respective areas, port safety and security and marine environmental protection regulations. There are 41 Captains of the Port nationwide.

[7] NVICs provide detailed guidance about enforcement or compliance with certain Coast Guard safety regulations and programs. NVIC 09–2, most recently revised on October 27, 2005, detailed requirements for area plans.

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

security-related disasters. 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, gives rise to 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, if ports take a system-wide approach, thinking strategically about using resources to mitigate and recover from all forms of disaster, they 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. Based on our 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 area committees and area plans to discuss all-hazards planning. While MTSA and its implementing regulations are focused on transportation security incidents rather than natural disasters and other types of emergencies, we believe that area plans provide a useful foundation for establishing an all hazards approach. Some federal officials indicated that separate existing plans can handle the range of threats that ports face. However, there would need to be an analysis of gaps between different types of planning. Finally, DHS noted that most emergency planning should properly remain with state and local emergency management planners and were cautious about the federal government taking on a larger role.

Maritime Security Exercises Require a Broader Scope and Participation

MTSA regulations require the Coast Guard Captain of the Port and the area committee to conduct or participate in exercises to test the effectiveness of area plans once each calendar year, with no more than 18 months between exercises. These exercises 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. Such exercises have been conducted for the past several years. For example, in fiscal year 2004, the Coast Guard conducted 85 port-based terrorism exercises that addressed a variety of possible scenarios. In August 2005, the Coast Guard and the Transportation Security Administration (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 expects to conduct PortSTEP exercises for 40 area committees and other port stakeholders.

The SAFE Port Act included several new requirements related to security exercises. It required 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 regulated by the MTSA. It 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. Finally, it added natural disasters, such as hurricanes or earthquakes, to be included in the list of scenarios to be tested.

Our work has not specifically examined compliance with these new requirements, but our review of these requirements and our work in examining past exercises suggests that implementing a successful exercise program faces several challenges.[9] These challenges include:

- **Setting the scope of the program.** It will be necessary to determine how exercise requirements in the SAFE Port Act differ from area committee exercises that are currently performed. Exercises currently conducted by area committees already test the ability of a variety of port stakeholders to work to-

[9] GAO, *Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention,* GAO–05–170 (Washington, D.C.: Jan. 14, 2005); *Maritime Security: Federal Efforts Needed to Address Challenges in Preventing and Responding to Terrorist Attacks on Energy Commodity Tankers,* GAO–07–286SU (Washington, D.C.: Mar. 20, 2007); *Port Risk Management: Additional Federal Guidance Would Aid Ports in Disaster Planning and Recovery,* GAO–07–412 (Washington, D.C.: Mar. 28, 2007).

gether in the event of a port incident. The potential exists for these efforts to be duplicated under the SAFE Port Act exercise requirements. On the other hand, the SAFE Port Act exercise requirements clearly move beyond previous requirements by including natural disasters and other emergencies in the list of scenarios to be exercised. Ensuring that these scenarios are exercised as part of a comprehensive security program may require a wider scope when exercise planning commences.

• **Completing after-action reports in a timely and thorough manner.** In past work, we found that earlier after-action reports were generally submitted late and that many failed to assess each objective that was being exercised. Inability to provide timely and complete reports on exercises represents a lost opportunity to share potentially valuable information across the organization as well as plan and prepare for future exercises.

• **Ensuring that all relevant agencies participate.** While exercise preparation and participation is time-consuming, joint exercises are necessary to resolve potential role and incident command conflicts as well as determine whether activities would proceed as planned. Our work has shown that past exercises have not necessarily been conducted in this manner.

Coast Guard Is in Process of Evaluating the Security of Foreign Ports

The security of domestic ports is also dependent on 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 their ports. The Coast Guard established this program, called the International Port Security Program, in April 2004. Under this program, 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.[10] 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.[11] As of April 2007, the Coast Guard reported that it has visited 86 countries under this program and plans to complete 29 more visits by the end of fiscal year 2007.[12]

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 timeframe for completion of these visits, the Coast Guard initially set a goal to visit all 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.[13] 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 these 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.

---

[10] 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, 2001, 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.

[11] 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.

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

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

We are currently conducting a review of the Coast Guard's international enforcement programs, such as the International Port Security Program.[14] Although this work is still in process and not yet ready to be included in this testimony, we have completed a more narrowly scoped review required under the SAFE Port Act regarding security at ports in the Caribbean Basin.[15] As part of this work, we looked at the efforts made by the Coast Guard in the region under the program and the Coast Guard's findings from the country visits it made in the region. For the countries in this region for which the Coast Guard had issued a final report, the Coast Guard reported that most had "substantially implemented the security code," while one country that was just recently visited was found to have not yet implemented the code and will be subject to a reassessment. At the facility level, the Coast Guard found several facilities needing improvements in areas such as access controls, communication devices, fencing, and lighting. Because our review of the Coast Guard's International Port Security Program is still ongoing, we have not yet reviewed the results of the Coast Guard's findings in other regions of the world.

While our larger review is still not complete, Coast Guard officials have told us they face challenges in carrying out this program in the Caribbean Basin. These challenges include:

- **Ensuring sufficient numbers of adequately trained personnel.** Coast Guard officials said the faster rate at which foreign ports will now be reassessed will require hiring and training new staff—a challenge they 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. Another related challenge is that the unique nature of the program requires the Coast Guard to provide specialized training to those joining the program, since very few people in the Coast Guard have had international experience or extensive port security experience.

Addressing host nation sovereignty issues. In making arrangements to visit the ports of foreign countries, Coast Guard officials stated that they have occasionally encountered initial reluctance by some countries to allow the Coast Guard to visit their ports due to concerns over sovereignty. In addition, the conditions of the visits, such as timing and locations, are negotiated between the Coast Guard and the host nation. Thus the Coast Guard team making the visit could potentially be precluded from seeing locations that were not in compliance.

Port Facility Security Efforts Are Long Standing, but Additional Challenges Have Emerged

Many long-standing programs to improve facility security at ports are underway, but new challenges to their successful implementation have emerged. The Coast Guard is required to conduct assessments of security plans and facility inspections, but faces challenges to staff and train staff to meet the additional requirements of the SAFE Port Act. 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 transportation workers are properly screened, but redundancies in various background checks have decreased efficiency and highlighted the need for increased coordination.

Coast Guard Faces Challenges in Monitoring Compliance of Maritime Facilities

MTSA and its implementing regulations requires owners and operators of certain at-risk maritime facilities (such as 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. Under the Coast Guard regulations, these plans are to include such items as measures for access control, responses to security threats, and drills and exercises to train staff and test the plan.[16] The plans are "performance-based," meaning 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. Facility owners were to have their plans in place by July 1, 2004.

---

[14] This work is being conducted at the request of the Committee on Commerce, Science and Transportation, U.S. Senate.

[15] Section 233 (c) of the SAFE Port Act requires GAO to report on various aspects relating to the security of ports in the Caribbean Basin. The act required GAO to provide this report to specified cognizant Senate and House Committees. To satisfy this requirement, GAO's findings for this work were presented in a briefing format to the cognizant committees by April 13, 2007. GAO will release a public report containing the briefing materials in June 2007.

[16] Requirements for security plans for facilities are found in 33 C.F.R. Part 105, Subpart D.

The Coast Guard performs inspections of facilities to make sure they are in compliance with their security plans. In 2005, we reported that the Coast Guard completed initial compliance inspections at all MTSA regulated facilities by the end of 2004 found that approximately 97 percent of maritime facility owners or operators were in compliance with MTSA requirements.[17] The most frequently cited deficiencies related to insufficient controls over access, not ensuring the facility was operating in compliance with security requirements, not complying with facility security officer requirements (such as possessing the required security knowledge or carrying out all duties as assigned), and having insufficient security measures for restricted areas. The Coast Guard reported taking enforcement actions and imposing operational controls, such as suspending certain facility operations, for identified deficiencies.

Coast Guard guidance calls for the Coast Guard to conduct on-site facility inspections to verify continued compliance with the plan on an annual basis. The SAFE Port Act required the Coast Guard to conduct at least two inspections of each facility annually, and it required that one of these inspections be unannounced. We are currently conducting a review of the Coast Guard's efforts for ensuring facilities' compliance with various MTSA requirements and are not yet in a position to report our findings.[18] However, our previous work showed the Coast Guard faces challenges in carrying out its strategy to review and inspect facilities for compliance with their security plans, and these challenges could be amplified with the additional requirements called for by the SAFE Port Act.[19] These challenges include:

- **Ensuring that sufficient trained inspectors are available.** Because security measures are performance-based, evaluating them involves a great deal of subjectivity. For example, inspectors do not check for compliance with a specific procedure; instead, they have to make a judgment about whether the steps the owner or operator has taken provide adequate security. Performance-based plans provide flexibility to owners and operators, but they also place a premium on the skills and experience of inspectors to identify deficiencies and recommend corrective action. This complexity makes it a challenge for the Coast Guard to ensure that its inspectors are trained appropriately and have sufficient guidance to make difficult judgments about whether owners and operators have taken adequate steps to address vulnerabilities. Additionally, once proficient at their job, inspectors often face reassignment. Further, the rotation period has been shortened by 1 year—from 4 years to 3.
- **Evaluating compliance activities so they can be improved.** In our previous work we also recommended that the Coast Guard evaluate its compliance inspection efforts taken during the initial 6-month period after July 1, 2004, and use the results as a means to strengthen its long-term strategy for ensuring compliance.[20] While the Coast Guard agreed with this recommendation, and has taken some steps to evaluate its compliance efforts, it has not conducted a comprehensive evaluation of these efforts to date. Without knowledge that the current approach to MTSA facility oversight is effective, the Coast Guard will be further challenged in planning future oversight activities.

TSA Has Made Progress in Implementing the TWIC Program, but Challenges Remain

MTSA required the Secretary of DHS to, among other things, issue a maritime worker identification card that uses biometrics, such as fingerprints, to control access to secure areas of seaports and vessels. When MTSA was enacted, TSA had already initiated a program to create an identification credential that could be used by workers in all modes of transportation. 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.

---

[17] See GAO, *Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges,* GAO–05–327 (Washington, D.C.: March 2005).

[18] This work is being conducted at the request of the Committee on Commerce, Science and Transportation, U.S. Senate.

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

[20] *Ibid.*

We have reported several times on the status of this program and the challenges that it faces.[21] 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.[22] 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 contained a requirement for implementing the first major phase of the TWIC program by mid-2007. More specifically, it 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. TSA is taking steps to address these requirements, such as establishing a rollout schedule for enrolling workers and issuing TWIC cards at ports and conducting a pilot program to test TWIC access control technologies.

As TSA begins enrolling workers and issuing TWIC cards this year, it is important that the agency establish clear and reasonable timeframes for implementing TWIC. Further, TSA could face additional challenges as the TWIC implementation progresses. These challenges include:

- **Monitoring the effectiveness of contract planning and oversight.** While the steps that TSA reports taking are designed to address the contract planning and oversight problems that we have previously identified and recommendations we have made, the effectiveness of these steps will not be clear until implementation of the TWIC program begins.
- **Ensuring a successful enrollment process.** Significant challenges remain in enrolling about 770,000 persons at about 3,500 facilities in the TWIC program. Sufficient communication and coordination to ensure that all individuals and organizations affected by the TWIC program are aware of their responsibilities will require concerted effort on the part of TSA and the enrollment contractor.
- **Addressing access control technologies.** TSA and industry stakeholders need to address challenges regarding TWIC access control technologies to ensure that the program is implemented effectively. Without fully testing all aspects of the technology TSA may not be able ensure that the TWIC access control technology can meet the requirements of the system. Given the differences among the facilities and locations where the technology is to be implemented, it may be difficult to test all scenarios.

Multiple Background Check Programs for Transportation Workers Need to Be Coordinated

Since the terrorist attacks on September 11, 2001, 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. For example, the USA PATRIOT Act in October 2001 prohibited states from issuing hazardous material endorsements for a commercial driver's license without an applicant background check.[23] Background checks are also part of the TWIC program discussed above. Concerns have been raised, however, that transportation workers may face a variety of background checks, each with different standards. A truck driver, for example, is subject to background checks for all of the following: unescorted access to a secure area at a port, unescorted access to a secure area at an airport, expedited border crossings, hauling hazardous materials, or hauling arms or ammunition for the Department of Defense or cargo for the U.S. Postal Service. 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.[24] The Commission recommended that a coordinating body raise standards, facilitate information-sharing, and survey systems for poten-

---

[21] 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).

[22] GAO, *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).

[23] Pub. L. No. 107–56, § 1012(a)(1), 115 Stat. 272, 396–97 (2001).

[24] *Final Report of the National Commission On Terrorist Attacks Upon that United States.*

tial problems. In August 2004, Homeland Security 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 has taken steps, both at the department level and within its various agencies, to consolidate, coordinate, and harmonize such background check programs.[25] At the department level, DHS created the Screening Coordination Office (SCO) in July 2006 to coordinate DHS background check programs. The 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. DHS components are currently in the initial stages of a number of their own 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.[26] 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 be submitted to TSA through the TWIC enrollment process.

The SAFE Port Act required us to conduct a study of DHS background check programs similar to the one required of truck drivers to obtain a hazardous material endorsement. Our work on other projects indicates that DHS is likely to face additional challenges in coordinating its background check programs. These challenges include:

- *Ensuring its plans are sufficiently complete without being overly restrictive.* The varied background check programs related to transportation workers may have substantially different standards or requirements. 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.
- **Ensuring that accurate performance information is available.** Without knowing the potential costs and benefits associated with the number of redundant background checks that would be eliminated through harmonization, DHS lacks the performance information that would allow its program managers to compare their program results with goals. Thus, DHS faces challenges in determining where to target program resources to improve performance. 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.
- **Coordinating across the broader universe of federal background check programs.** Many other federal agencies also have background check programs, making coordination a cross-cutting, government-wide issue. DHS could face challenges harmonizing background check programs within DHS and other federal agencies.

container Security Programs Maturing, but Implementation Challenges Continue

Several container security programs have been established and matured through the development of strategic plans, human capital strategies, and performance measures. But these programs continue to face technical and management challenges in implementation. As part of its layered security strategy, CBP developed the Automated Targeting System, but this system has faced quality assurance challenges since its inception. In the past, CSI has lacked sufficient staff to meet requirements. C–TPAT has faced challenges with validation quality and management in the past, in part due to its rapid growth. DOE's Megaports Initiative faces ongo-

[25] See GAO, *Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges,* GAO–05–327 (Washington, D.C.: March 2005).

[26] TSA determined that the background checks required for the hazardous materials endorsement, which authorizes an individual to transport hazardous materials for commerce; and the Free and Secure Trade card, a voluntary CBP program for 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 Feb. 3, 2003, and Mar. 26, 2007) was not subject to an additional background check for TWIC.

ing operational and technical challenges in the installation and maintenance of radiation detection equipment at ports.

Automated Targeting System Continues to Require Management Action

As part of its responsibility for preventing terrorists and weapons of mass destruction from entering the United States, CBP addresses potential threats posed by the movement of oceangoing containers. CBP inspectors at seaports help determine which containers entering the country will undergo inspections and then perform physical inspections of such containers. To carry out this responsibility, CBP uses a layered security strategy that attempts to focus resources on potentially risky cargo containers while allowing other cargo containers to proceed without disrupting commerce. The ATS is one key element of this strategy. CBP uses ATS to review documentation, including electronic manifest information submitted by the ocean carriers on all arriving shipments, to help identify containers for additional inspection.[27] 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. ATS is a complex mathematical model that uses weighted rules that assign a risk score to each arriving shipment based on manifest information. CBP inspectors use these scores to help them make decisions on the extent of documentary review or physical inspection to conduct.

In our previous work on ATS we found that CBP lacked important internal controls for the administration and implementation of ATS.[28] Despite ATS' importance to CBP's layered security strategy, CBP was still in the process of implementing the following key controls, (1) performance metrics to measure the effectiveness of ATS, (2) a comparison of the results of randomly conducted inspections with the results of its ATS inspections, and (3) a simulation and testing environment. At that time CBP was also in the process of addressing recommendations contained in a 2005 peer review.

The SAFE Port Act required that the CBP Commissioner take actions to improve ATS. These requirements included such steps as (1) having an independent panel review the effectiveness and capabilities of the ATS, (2) considering future iterations of ATS that would incorporate smart features, (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 Inspector General of the Department of the Treasury and DHS. Based on our findings and the further changes to the program enacted by the SAFE Port Act, we found the following challenge faced by CBP:

• **Implementing the program while internal controls are being developed.** The missing internal controls would provide CBP with critical information on its container screening performance. CBP's vital mission does not allow it, however, to halt its screening efforts during the period it needed to put these controls into place. CBP is faced with the challenge of ensuring that the highest-risk containers are inspected without important information needed for optimum allocating resources used targeting and inspecting containers.

The CSI Program Has Matured but Challenges Remain

In response to the threat that a cargo container could be used to smuggle a weapon of mass destruction (WMD) into the United States, the U.S. Customs Service (now CBP) initiated the CSI in January 2002 to detect and deter terrorists from smuggling WMDs via containers before they reach domestic seaports. Under this initiative, foreign governments allow CBP personnel to be stationed at foreign seaports to identify container shipments at risk of containing WMD. CBP personnel refer high-risk shipments to host government officials, who determine whether to inspect the shipment before it leaves for the United States. Host government officials examine shipments with nonintrusive inspection equipment and, if they deem it necessary, open the cargo containers to physically examine the contents inside.[29]

---

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

[28] 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).

[29] A core element of CSI is the use of technology to scan 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.

Since our last report on the CSI program, CBP has increased the number of seaports that participate in the program from 34 to 50, with plans to expand to a total of 58 ports by the end of this fiscal year.[30]

In our previous work, we identified numerous issues affecting the effectiveness of the CSI program. On the positive side, we praised some of the positive interaction and information sharing we found among CBP officials and host nation officials at CSI ports—something that could lead to better targeting and inspections. In some cases where we found problems, CBP took steps to implement our recommendations, such as developing a strategic plan, a human capital strategy, and performance measures. In other cases, CBP found it more difficult to implement our recommendations. For example, they deferred establishing minimum technical requirements for nonintrusive inspection equipment used by host nations at CSI ports.

The SAFE Port Act formalized CSI into law and specified factors to be considered in designating seaports as CSI, including risk level, cargo volume, results of Coast Guard assessments, and the commitment of the host government to sharing critical information with DHS. The act also called for DHS to establish minimum technical criteria for the use of nonintrusive inspection equipment in conjunction with CSI and to require that seaports receiving CSI designation operate such equipment in accordance with these criteria. Another provision related to container cargo requires DHS to ensure that integrated scanning systems, using nonintrusive imaging equipment and radiation detection equipment, are fully deployed to scan all containers before their arrival in the United States as soon as possible, but not before DHS determines that such systems meet a number of criteria. The SAFE Port Act addresses a number of the issues we have previously identified, but our work suggests that CBP may face continued challenges going forward. These challenges include:

- **Ensuring sufficient staff are available for targeting.** Although CBP's goal is to target all U.S. bound containers at CSI seaports before they depart for the United States, we previously reported that it has not been able to place enough staff at some CSI ports to do so.[31] Since then, CBP has provided additional support to deployed CSI staff by using staff in the United States (at the National Targeting Center) to screen containers for various risk factors and potential inspection.
- **Developing an international consensus on technical requirements.** There are no internationally recognized minimum technical requirements for the detection capability of nonintrusive inspection equipment used to scan containers. Consequently, host nations at CSI seaports use various types of nonintrusive inspection equipment and the detection capabilities of such equipment can vary. Because the inspection a container receives at a CSI seaport could be its only scan before entering the United States, it is important that the detection equipment used meets minimum technical requirements to provide some level of assurance that the presence of WMDs can be detected.
- **Ensuring that designated high-risk containers are inspected.** We also found that some containers designated as high risk did not receive an inspection at the CSI seaport. Containers designated as high risk by CSI teams that are not inspected overseas (for a variety of reasons) are supposed to be referred for inspection upon arrival at the U.S. destination port. However, CBP officials noted that between July and September 2004, only about 93 percent of shipments referred for domestic inspection were inspected at a U.S. seaport. According to CBP, it is working on improvements in its ability to track such containers to assure that they are inspected.

DOE Has Made Progress with Megaports Program

Another component in the efforts to prevent terrorists from smuggling weapons of mass destruction in cargo containers from overseas locations is the Megaports Initiative, initiated by the Department of Energy's (DOE) National Nuclear Security Administration in 2003. The goal of this initiative is to enable foreign government personnel at key 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.

---

[30] 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).

[31] GAO–05–557.

Through April 2007, DOE had completed installations of radiation detection equipment at nine ports: Freeport, Bahamas; Piraeus, Greece; Puerto Cortes, Honduras; Rotterdam, the Netherlands; Port Qasim, Pakistan; Manila, the Philippines; Port of Singapore; Algeciras, Spain; and Colombo, Sri Lanka. Additionally, DOE has signed agreements to begin work and is in various stages of implementation at ports in 15 other countries: Belgium, Columbia, China, the Dominican Republic, Egypt, Israel, Jamaica, Mexico, Oman, Panama, South Korea, Taiwan, Thailand, the United Arab Emirates, and the United Kingdom. Further, in an effort to expand cooperation, DOE is engaged in negotiations with approximately 20 additional countries in Europe, Asia, the Middle East, and South America.

When we reported on this program in March 2005, DOE had made limited progress in gaining agreements to install radiation detection equipment at the highest priority seaports.[32] At that time, DOE had completed work at only two ports and signed agreements to initiate work at five other ports. 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, its physical layout, and existing infrastructure. Since our review, DOE has developed a strategic plan for the Megaports Initiative and is in the process of revising its per port cost estimate.

As DOE continues to implement its Megaports Initiative, it faces several operational and technical challenges specific to installing and maintaining radiation detection equipment at foreign ports. These challenges include:

- **Ensuring the ability to detect radioactive material.** Certain factors can affect the general capability of radiation detection equipment to detect nuclear material. For example, some nuclear materials can be shielded with lead or other dense materials to prevent radiation from being detected. In addition, one of the materials of greatest proliferation concern, highly enriched uranium, is difficult to detect because of its relatively low level of radioactivity.
- **Overcoming the physical layout of ports.** In its effort to screen cargo containers at foreign ports for radioactive and nuclear materials, DOE faces technical challenges related to these ports' physical layouts and cargo stacking configurations. To address a part of these challenges at some ports, DOE is testing at Freeport, Bahamas, a device used to transport cargo containers between port locations—known as a straddle carrier—that is outfitted with radiation detection equipment.
- **Sustaining equipment in port environments.** Additionally, environmental conditions specific to ports, such as the existence of high winds and sea spray, can affect the radiation detection equipment's performance and long-term sustainability. To minimize the effects of these conditions, DOE has used steel plates to stabilize radiation portal monitors placed in areas with high winds, such as in Rotterdam, and is currently evaluating approaches to combat the corrosive effects of sea spray on radiation detection equipment.

Secure Freight Initiative Only Recently Announced

In another provision related to container security and the work to address WMD and related risks, the SAFE Port Act specified that new integrated scanning systems that couple nonintrusive imaging equipment and radiation detection equipment must be pilot tested at three international seaports. 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 such ports. To fulfill these requirements, DHS and DOE jointly announced the formation of a pilot program called the Secure Freight Initiative (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.

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

[32] 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).

are: Port Qasim in Pakistan; Puerto Cortes in Honduras; and Southampton in the United Kingdom. Three other ports located in Singapore, the Republic of Korea, and Oman will receive more limited deployment of these technologies as part of the pilot program. According to DHS, 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. The determination about what containers are inspected will be made by CBP officials, either on the scene locally or at CBP's National Targeting Center.

We have not yet reviewed the efforts made under SFI. However, in carrying it out, the agencies may likely have to deal with the challenges previously identified for the CSI and Megaports programs. Per the SAFE Port Act, DHS 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, and every 6 months thereafter, DHS 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.

C–TPAT Maturing, but Validation and Other Management Challenges Remain C–TPAT, initiated in November 2001, is designed to complement other container security programs as part of a layered security strategy. 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 improving the security of their shipments by joining the program, C–TPAT members receive benefits that result in reduced scrutiny of their shipments, such as a reduced number of inspections or shorter wait times for their shipments. Since C–TPAT's inception, CBP has certified 6,375 companies, and as of March 2007, it had validated the security of 3,950 of them (61.9 percent).

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 the company 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 our previous work, we raised a number of concerns about the overall management of the program and the effectiveness of the validation process.[33] We found that CBP had not established key internal controls necessary to manage the programs. Since that time, CBP has worked to develop a strategic plan, a human capital strategy, and performance measures. We also found that validations lacked sufficient rigor to meet C–TPAT stated purpose of the validations—to ensure that members' security measures are reliable, accurate and effective. Since that time, CBP has developed new validation tools, and we have ongoing work to assess what progress is being made.

The SAFE Port Act formalized C–TPAT into law. In addition, it included a new goal that CBP 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. CBP faces several challenges in addressing this requirement and dealing with the concerns we previously identified. These challenges include:

- Conducting validations within 1 year. The goal of completing validations within a year of members' certification is a challenge. While CBP has belatedly reached some of its earlier staffing goals, consistent membership growth has led to a steady backlog of validation requirements.
- **Ensuring sound validations.** CBP's standard for validations—to ensure that members' security measures are reliable, accurate and effective—is hard to

[33] 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).

achieve. Since C–TPAT is a voluntary rather than a mandatory program, there are limits on how intrusive CBP can be in its validations. Further, CBP lacks jurisdiction over foreign companies operating outside the United States in a member's foreign supply chain; therefore its ability to review the complete supply chain of a member is questionable.

• Measuring outcomes and results. Challenges developing C–TPAT outcome-based performance measures persist because of difficulty measuring deterrent effect. CBP has contracted with the University of Virginia for help in developing useful measures.

DHS's Emphasis on Security Issues Has Contributed to Diminished Attention on Customs Revenue Functions

While DHS's priority mission since its inception has been homeland security, various DHS components have other nonsecurity functions. CBP, which is responsible for border security, also collects customs duties and other revenues. In forming DHS, there was concern that moving the customs revenue functions from Treasury into the new CBP would diminish attention given to these functions. In recognition of that concern, Congress required the newly created DHS not reduce the number of staff in key positions related to customs revenue functions.[34] CBP is the second largest revenue generator for the U.S. government, collecting nearly $30 billion in customs revenue in fiscal year 2006. The SAFE Port Act required us to study the extent to which CBP had been able to carry out its customs revenue functions. We recently completed this study,[35] in which we found three key weaknesses related to CBP's performance of customs revenue functions: (1) CBP failed to maintain the legislatively mandated staffing levels for performing customs revenue functions, (2) CBP lacks a strategic workforce plan to help ensure it has a sufficient number of staff with the necessary skills and competencies to effectively perform customs revenue functions, and (3) CBP does not publicly report on its performance of customs revenue functions, which would help ensure accountability.

Although Improving, CBP Failed to Maintain Mandated Staffing Levels for Customs Revenue Positions

Staff resources contributing to customs revenue functions generally declined since the formation of DHS in March 2003, in part due to department priorities focused on homeland security and recruiting and retention problems for some positions. As shown in figure 1, since September 2003, CBP has not maintained the mandated number of staff in each of the nine designated customs revenue positions, although recent efforts by CBP increased the number of staff to the mandated levels in most of these positions as of December 2006. For example, the number of Import Specialists on board dropped from 984 in March 2003 to a low of 892 in March 2006, and grew to 1,000 in December 2006. CBP was below the mandated staff levels for three customs revenue positions as of December 2006, ranging from 2 to 34 positions below the baseline. Recently, CBP took several steps such as opening job announcements and closely monitoring its customs revenue staffing levels to increase the number of customs revenue staff by more than 130 to 2,273.[36]

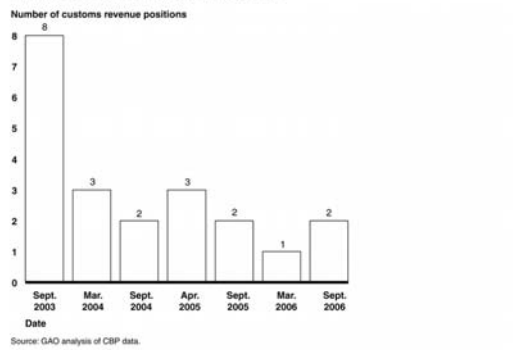
---

[34] The Homeland Security Act of 2002 (Pub. L. No. 107–296, Sec. 412, 116 Stat. 2135, 2179) required DHS to maintain a least the March 2003 number of staff in each of nine specific customs revenue positions and their associated support positions. The nine designated customs revenue positions are Import Specialists, Fines and Penalties Specialists, attorneys of the Office of Regulations and Rulings, Customs (Regulatory) Auditors, International Trade Specialists, and Financial Systems Specialists. When DHS was formed in March 2003, it employed 2,263 people in customs revenue positions and 1,006 additional associated support staff.

[35] GAO, *Customs Revenue: Customs and Border Protection Needs to Improve Workforce Planning and Accountability,* GAO–07–529 (Washington, D.C.: Apr. 12, 2007).

[36] See appendix I for more information on staff levels over time. I21The number of support staff—which includes a variety of management, technical, and administrative support positions—associated with the customs revenue positions has also declined overall, and the declines for some positions have been substantial. For example, the Import Specialist position lost 94 of its 407 mandated level for support staff. As shown in figure 2, CBP has maintained the mandated support staff levels for few of the customs revenue positions, with six of eight positions being below the mandated level in September 2006.

Figure 2: Number of Customs Revenue Positions for Which CBP Has Maintained Mandated Associated Support Staffing Levels



Source: GAO analysis of CBP data.

Lastly, other positions within DHS such as CBP Officers, Immigration and Customs Enforcement (ICE) Investigators, and Office of Inspector General (OIG) Auditors contribute to performing or improving customs revenue functions, but their contributions have declined over time. For example, before the formation of DHS, there were about 65 Treasury OIG Auditors focused on customs issues. Since the formation of DHS, the DHS OIG has prioritized audits in other areas such as homeland security and, more recently, disaster assistance, and the number of Auditors focusing on customs issues declined to 15 as of February 2007. Because of other priorities, DHS OIG Auditors have not conducted any assessments of high-risk areas within customs revenue functions and have not done any performance audits focused on improving these functions.

CBP Lacks a Strategic Workforce Plan, but Some Steps Taken to Improve Its Human Capital Management as It Faces Key Challenges

CBP lacks a strategic workforce plan to guide its efforts to perform customs revenue functions but has taken some recent steps to improve its human capital management amid external and internal challenges. CBP has not performed an assessment to determine the critical workforce skills and competencies needed to perform customs revenue functions. In addition, CBP has not yet determined how many staff it needs in customs revenue positions, their associated support positions, and other positions that contribute to the protection of customs revenue. Further, CBP has not developed a strategic workforce plan to inform and guide its human capital efforts to perform its current and emerging customs revenue functions. CBP has recently taken some steps to improve staffing for customs revenue functions, but gaps exist in these efforts. CBP has proposed revising the roles and responsibilities for Import Specialists and is working to develop legislatively mandated resource allocation models to determine ideal staffing levels for performing various agency functions. For example, the SAFE Port Act requires CBP to determine optimal staffing levels required to carry out CBP's commercial operations. According to CBP, this model, which is due in June 2007, will suggest the ideal staffing level for the customs revenue positions as well as some other trade-related positions. However, the resource allocation models being developed will not assess the deployment of customs revenue staff across the more than 300 individual ports—an important consideration since about 75 percent of customs revenue staff work at ports of entry.

Additionally, external and internal challenges heighten the importance of such strategic workforce planning. First, the workload for some customs revenue positions has increased. For example, the growing number of free trade agreements has had a pronounced effect on some customs revenue positions, including attorneys in CBP's Office of Regulations and Rulings who participate in every phase of the negotiation and implementation of the free trade agreements—from participating in negotiating sessions through issuing binding rulings regarding the proper interpretation of the CBP regulations implementing the agreement. In addition, some customs revenue positions have seen an expansion of revenue-related as well as nonrevenue-related responsibilities. For instance, with the formation of DHS, the Fines, Penalties, and Forfeitures Specialists from the former Customs Service became responsible for administering fines and penalties for violations of immigration and agriculture laws in addition to their existing responsibilities related to customs law. Also, staff in some customs revenue positions told us they have been assigned work

that is unrelated to customs revenue functions. For example, one port has not had a Secretary/Receptionist position for 5 years. As a result, that function was given to Import Specialists on a rotational basis.

CBP's Public Reporting Does Not Ensure Accountability for Customs Revenue Functions

Despite being the second largest revenue generator for the U.S. government, CBP does not publicly report on its performance of customs revenue functions in its annual plans and performance reports, thus failing to help ensure accountability. We have previously found that good management practices dictate linking performance measures to strategic goals and objectives in an effort to improve performance and accountability. Good management practices also suggest publicly reporting this information so that Congress can make informed decisions and so that taxpayers have a better understanding of what the government is providing in return for their tax dollars, or in this case, how well it is collecting customs revenue. CBP's strategic planning documents recognize the importance of customs revenue protection by establishing it as a strategic objective and identifying a revenue-related performance measure. However, we found that CBP does not use this measure or publicly report on results related to its customs revenue functions in its annual plans and Performance and Accountability Reports, the official documents agencies issue to Congress and the public to report program performance. According to a CBP official, CBP does not report on customs revenue functions in its Performance and Accountability Reports because these functions do not directly address its long-term goal of facilitating trade.

In our recent report, we made three recommendations. We recommended that the CBP Commissioner develop a strategic workforce plan and work with the Office of Management and Budget to establish and report on performance measures related to customs revenue functions in its Performance and Accountability Reports. We also recommended that the DHS Inspector General should identify areas of high risk related to customs revenue functions. The department concurred with our recommendation to develop a strategic workforce plan and partially concurred with our recommendation to establish and report on specific customs revenue performance measures and agreed to take action to implement these recommendations by March 31, 2008. The DHS Inspector General also concurred with our recommendation and agreed to take action to implement it by September 30, 2007.

Concluding Observations

MTSA established a maritime security framework that the Coast Guard implemented with area maritime security committees, area maritime security plans, and exercises to test the plans. In addition, various agencies showed initiative in establishing other programs related to maritime security—such as the Coast Guard, DOD and DOJ establishing interagency operations centers; CBP implementing CSI and C–TPAT; and DOE establishing the Megaports Inititive. In some cases, agencies have struggled to implement programs required by MTSA or other legislation—such as TSA delays with the TWIC program and CBP not meeting required staffing levels for customs revenue functions. The SAFE Port Act further defined and strengthened this maritime security framework—and created additional requirements for agencies at a time when their programs are still maturing. We have reviewed many of the MTSA and SAFE Port Act related programs and made recommendations 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. We will continue to monitor these programs and provide Congress with oversight and insight into maritime security.

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

For Information about this testimony go to caldwells@gao.gov.

Ms. SANCHEZ. Thank you, Mr. Caldwell.

Now I will give myself some time in order to ask my questions, and then we will move on to the ranking member.

Let's see, to the TWIC lady, do I have anything for you?

[Laughter.]

Welcome, by the way.

According to the SAFE Port Act, TSA is supposed to begin the TWIC at the top 10 ports. Can you provide us with the names of those ports? And how did you select those ports?

Ms. FANGUY. We have actually just recently published the list of the 130 initial list of fixed-enrollment sites, so those are the different ports. We are still working with our program to finalize the deployment plan. At this time, we are working through the testing of the overall TWIC program.

So, again, as I said in my opening statement, we want to make sure that we get the program right. We are still planning on starting at Wilmington. That has been our plan. We continue to have that as our plan. After we field test our processes in Wilmington, we will be progressing out throughout the nation at the rest of the 129 ports.

Ms. SANCHEZ. Last week we heard that—well, before last week, when we had that briefing, some of our staff was talking to some of the Homeland staff about when we would meet that deadline, because it is set for July 1. We were told that it might be until September. Then last week we heard you were trying to meet that July 1 deadline.

What do you think is happening over there? Because you really haven't even picked the 10 ports. You can't tell them to me today. I know what you just told me. I have it in front of me, but that doesn't really answer my question.

Ms. FANGUY. Sure. Again, we are continuing to test the TWIC program. We want to make sure that on the five key areas I talked about that we absolutely get those pieces right. We need to make sure that the data for TWIC applicants is processed correctly through all five of those key components. And that when they work together, that they tie the security threat assessment data to the right individual. Then when that credential is used at a port facility, that again it can be used to tie the information back to that individual.

Again, we want to get it right so that we don't impact commerce and we don't impact people's livelihoods.

Ms. SANCHEZ. I understand that answer, but that is not the answer to the question that I asked.

Ms. FANGUY. We are continuing to try to move the program out as aggressively as possible, while very much focusing on program integrity.

Ms. SANCHEZ. So does that mean July 1 or not?

Ms. FANGUY. We are very focused on the July 1 deadline, but again, we want to definitely focus on program integrity to make sure that we get the program right the first time.

Ms. SANCHEZ. And how about the top 10 ports? Can you list them today?

Ms. FANGUY. I cannot list them for you today.

Ms. SANCHEZ. Okay. Can you give us some information on how TSA selected Lockheed as the prime contractor? It is also my understanding that there is at least one company that protested the decision. How is that going to impact our timeline in trying to get this done?

Ms. FANGUY. Sure. Let me address the second part first. I am actually very pleased to announce that the company that had pro-

VerDate Nov 24 2008 13:52 Jun 18, 2009 Jkt 000000 PO 00000 Frm 00053 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-31\48906.TXT HSEC PsN: DIANE

tested the TWIC award worked through the Federal Aviation Administration's Office of Dispute Resolution for Acquisitions, and that protest has now been resolved. So we are very pleased about that, so that should not impact Lockheed Martin's overall timeline.

In terms of the Lockheed Martin selection, when we set about putting together the RFP for the TWIC program, we were looking at two key factors. The first is to make sure that we had a company that has the appropriate skills and resources to manage a technology system of the scale and complexity of the TWIC program. So again, we were looking for a technology that had the right resources there.

The other piece of it, of course, is the deployment. That is absolutely critical to the TWIC program. So we were looking for a company that had a flexible approach to rolling out the program; a company that would actually have the resources to be able to go out at the minimum of 130 locations, but essentially have the flexibility to offer more flexible options to make things more convenient for our port workers.

So Lockheed Martin had a very flexible plan. They are going to be going to those 130 locations. They have a flexible contract structure so that we can add additional locations if appropriate. And then they will also be doing mobile enrollment. So those are some of the things that we looked at, and we really liked their proposal and we are very excited to work with them as we move forward in the TWIC program.

Ms. SANCHEZ. Do they know the top 10 ports?

Ms. FANGUY. They are working at our direction on the top 10 ports.

Ms. SANCHEZ. Okay.

One quick question for the admiral, and then I have one for Mr. Ahern. I have a lot for you, but I am going to let the rest of my colleagues go for a moment.

On long-range vessel tracking, you said we have all the data, but there is a problem in how we manipulate it, get it together, and have access to the right people for it. Does that mean that the Coast Guard's people in the field are unable to access on the information that they need to do their job?

Admiral BONE. Madam Chairwoman, the reality is we know exactly where vessels are, and we actually do work, again, interagency, both within DHS, but also in the intelligence committee and other sources to gather information on it. What is important, though, is how you collectively respond and do that in the most timely manner, and fuse that information so that you put the resources to it in a timely manner and most effective manner.

We know we can make improvements in that area. We also can make improvements in the way we communicate with the maritime industry what our intent is going to be, when we are going to take action with a vessel and the basis for it, and basically taking information that may even be coming in in a classified manner, and moving it into a law enforcement-sensitive so that we can communicate and set expectations.

The marine industry quite often is concerned about predictability and timing issues, and the costs associated with delays. I think as we improve our processes and improve our capabilities with the fu-

sion of that information and communication, we will be better able to use our shared interagency resources and set expectations for the marine industry.

Ms. SANCHEZ. How are you currently using the Maritime Information Service of North America? And could that help the process? Is there no overlap there? What is going on with that?

Admiral BONE. We actually procure data from a variety of sources, including MISNA. In fact, in areas where there are gaps of information or there are gaps related into our sensor technology, or whether it is the best return on investment to the government to use those services, we will acquire those services. That is an example.

I would offer that those services also, whether or not they are purchased, are extremely useful and have proven useful in responses to incidents in order to control and manage traffic in areas where there are no vessel traffic systems in place, and even in places where there are vessel traffic systems, to communicate to the industry as well as communicate across the government sectors in some of the hard-to-reach places such as Alaska and the Northwest.

I think we need to figure out how to best use all the marine exchanges, both in prevention, but I can tell you both in response and recovery and even continuity of operations. I know the Port of L.A.–L.B. is about to undertake an exercise looking at continuity of operations following a significant event. I think the Marine Exchanges provide an essential service in that operation as well.

Ms. SANCHEZ. Thank you, Admiral.

Mr. Ahern, I have a question about the empty container pilot, because my main concern when we were envisioning this was, being from the West ports, all the empties that arrive to the port and then sit around. Which government agency has the information on how many empties sit at particular ports?

Mr. AHERN. I can tell you as far as the universe of empty containers that come into the country internationally from abroad, there are 461,650. That would be an international responsibility that we would have within Customs and Border Protection.

Ms. SANCHEZ. But those are ones that are coming in.

Mr. AHERN. That would be correct.

Ms. SANCHEZ. What about ones that are coming from areas, say, they brought something in from China and now they have put them at the Wal-Mart in the middle of the country or whatever; and now we have to get that container back on that ship and it is going to go empty. Does anybody keep numbers on where those empties are at any time?

Mr. AHERN. Those would basically be in the custody and control of the carrier at that point in time, or if they are subletting those out to individuals. But the universe we are responsible for are the international arrivals that come from foreign ports, and that is that 461,000 universe.

Ms. SANCHEZ. Do you have any idea how long empty containers that are delivered from land-side to the ports sit around?

Mr. AHERN. I don't have any data on that.

Ms. SANCHEZ. Can you tell me what you think is the mean or what did it look like, or is there a program to look at these empty containers when they come from land-side?

Mr. AHERN. That would not be something that we are looking at within Customs and Border Protection. I would tell you some of the things that we are doing, and what our part of the SAFE Port Act requirements that we are looking at as part of the pilot if you would like.

Ms. SANCHEZ. Thank you.

To my ranking member, Mr. Souder.

Mr. SOUDER. I don't want you to get offended if I don't ask lots of questions to each one of you, because I have so many I can't possibly cover them.

The last round of questioning sounded like the entry/exit on the border with humans, and it is something we are going to need to look at because it is a potential vulnerability. Just out of curiosity, is anybody watching it?

I am not familiar enough with this TWIC port targeting. Why is it hard to say the 10 that you are going to? I missed it. Why can't you just say these are the 10. Wouldn't they be the 10 largest?

Ms. FANGUY. In terms of the overall deployment plan, we are starting at Wilmington. They were one of our prototypes since they know the program pretty well, and we have been working very closely with them to prepare for the start of TWIC enrollment.

In terms of the remaining ports, what we are looking at is port criticality, size of ports, but then we are also looking at the overall deployment approach and taking industry best practices to make sure that we don't want to start at the very largest ports first because potentially it could negatively impact commerce there.

So what we are going to do is have a mix of large and small ports as we go out across the nation. That is going to allow us to field test the overall processes.

So we are going to front-load the most critical ports in our overall deployment plan, but when we do put out our deployment plan, you are going to see a mix, again, of smaller and larger ports as we fan out across the nation.

Mr. SOUDER. I kind of understand that, but not completely, because Wilmington is supposed to be the test, and what you are telling me is that you are not confident enough in the test to have it be at the largest and most critical ports because it could foul up commerce, but that was supposed to be resolved in a test.

Let me ask each of our government witnesses, Admiral and Mr. Ahern and Ms. Fanguy, do you agree with Mr. Caldwell that you have had an expansion of tasks and resources haven't matched?

Admiral BONE. Congressman, this is a situation where, how much risk do you want to buy down? How much vulnerability do you want to close? As you identified, there are things that you can do, and one of our biggest jobs every day is to take the government's dollars and the taxpayer's dollars, I should say, and make the best use of it.

I can tell you that surely if you gave the Coast Guard, TSA or Customs and Border Protection more funding and resources, we could close more vulnerabilities and reduce the risk to the public, more so than we will be able to today.

Mr. SOUDER. Thank you. That was a great answer on the confines of what government witnesses have.

Mr. Ahern?

Mr. AHERN. Would it surprise you if I stay within those same confines?

[Laughter.]

I would first want to begin by thanking this Congress for providing what we did receive in fiscal year 2007. We received a plus-up of around 556 positions, principally dedicated for our seaports and principally to use for the radiation portal monitors and the large-scale X-ray systems we have deployed over the last 2 and 3 years.

One of the things as you deploy technology, oftentimes we don't forecast quickly enough or have the opportunity to get the commensurate level of resources it takes to man and follow up on alarms, anomalies and things of that nature that comes with the technology. For instance, for the radiation portal monitors, since we deployed close to 1,000 RPMs now at our northern and southern borders in a maritime environment, we have run over 151 million transactions through those RPMs.

That is great for the security of the country, and we will continue to do that, but the resolution of those alarms has been to the tune of over 800,000 alarms that we have had to resolve, thereby consuming a lot of resources to do that. So we are very pleased to receive the resources we did get this year. As we continue to deploy, we need to make sure that as we are modeling not only the needs for technology, but also what it takes in resources to run those.

Mr. SOUDER. Ms. Fanguy, let me make yours even more specific. If you had more resources, would you be closer to making the deadline goals?

Ms. FANGUY. In terms of this, this is one of those cases where again on technology, you want to make sure that you go through it, and it takes a certain amount of time.

So again, it takes 9 months to make a baby, which is very close to my mind because I just had a baby. So this is one of those things where we want to get this right. We want to make sure that the technology has been fully tested before we put it out there in the port environment.

Mr. SOUDER. So it is not a financial constraint that has restricted your testing? In other words, if we doubled your money would you get it into the experimental ports faster?

Ms. FANGUY. You could certainly do lots and lots of tests and lots and lots of testing. With more money, you can do lots of tests. But in terms of getting it out there, we are looking at more overall entry and exit criteria as we go through the phases of testing. So what I mean by that is we lay out objective criteria when we start a phase of testing, and we lay out the exit criteria. So we say, these are the types of errors that we cannot have as we come out of the tests.

So as an example, it is absolutely unacceptable not to have the security threat assessment go to all of the different vetting sources that we need it to go to. That has to be met. So that is what we are looking at in terms of the overall testing program. Again, we want to make sure that we get it right.

Mr. SOUDER. It is a fundamental question, because I have many of these electronics companies in my area who are actually working with Homeland Security on some of these IDs. And obviously the more places you test and the more tests you have, the more you find out what is working and not working. It becomes tough to make deadlines if we haven't put adequate funds in to getting all that process through.

Let me ask Mr. Ahern another question along the same lines. Do you feel pretty comfortable that in our risk-based container checking of known shippers, containers that seem to be at risk, anomalies, that we are in effect getting 100 percent screening of the highest risk, along with a high-percent at random to double check that?

Mr. AHERN. I am very comfortable with the layered strategy that we do have, but I would submit that what we need to do is continue to build upon the current layers we have. One of the things I spoke about that also is a requirement under the SAFE Port Act is getting additional information that we can then run through our targeting mechanism, the automated targeting system. We are in the process of doing that.

We have been working exhaustively with stakeholders, the trade, and the carrier community, to try to get 10 data elements, plus two additional. And to the chairwoman's question on the empty containers, one of the things that we will be looking for is being referred to as "10 plus 2," it is ten data elements additional that we are going to get deeper into the supply chain for being able to validate the information.

But also, one of the two elements will be container status messages, which will be provided to us so that we actually can be able to track and monitor the container movements when they are coming in and out of gates globally. So that will give us some visibility as far as just to be able to pinpoint and track a lot of these containers going forward. But we will be in the rulemaking process on that coming up in the next few weeks, and we will go forward with the public comment period.

Mr. SOUDER. One of my concerns is that I have seen, for example, Long Beach-Los Angeles is our biggest port. Over the number of years that I have been in Congress going several times before 9/11 and since, is steady improvement in perimeter security, I think 100 percent radiological screening there. And we have certain basic general improvements.

But that 100 percent container screening, when we are already resource-challenged, when we still don't have clear resolutions to chem-bio screening and need tremendous resources there, where the locks on the containers are still a question. The containers coming back in is a question; getting adequate screening so we don't have penetration into the people who are working at the places.

It seems to me that on the container side, we are ramping up, but if we are not careful, we are going to have a limited resource switching to something that is low risk, and take it from high risk, not to mention from narcotics. And that was partly some of my questioning, because this is difficult, where even if we increase the resources substantially, the combination of the missions and the things where we still have vulnerabilities are huge.

One last thing, and this was one of the most amazing things that I have seen. I have seen at the ports the different testing, but I was up at the Soo border, the Michigan-Soo-Canada, and was in the little station. And the person comes through and a little radiation beep went off. I thought I am either dead or I don't know what is going on here. But the beeper went off, and obviously they had seen this before because they asked the person, "Did you just have an operation?" And he said, "Why? Did something go off in there?" They said, "You need to get to secondary immediately."

They got him out of his vehicle, tested the vehicle—no radiation. They put the radiation monitor on him, and not only did it identify it, because he said "I had an operation 10 days ago." It said the date and it said the name of the form of volume and the amount in him. And he said both as they first pulled him over, and there he said, "I right now am more impressed with the United States homeland security program than I have ever been in my life. I can't believe you identified that 10 days ago I had an operation, and I have a little bit of radiation in my body."

We have made improvements, and we just need to get, in many of our opinions, accelerate that progress.

Mr. AHERN. I would like an opportunity to answer. I think it is a great question and a great point.

Finishing on the last point first, I actually had that personal experience. I had had a thallium stress test about 2 years ago. I had to go to Canada for a meeting and came back through the radiation portal on primary. It was about 10 days after the stress test, and the thallium isotope still did alert to me on primary as I walked in. We resolved the issue, but I had a chance to actually red test our own operation first hand.

But all that being said, to your point, I think there is a very good discussion we need to have as a government, and certainly with this Congress and this subcommittee as we move forward in the future. We have had, as I stated in my short statement, a very well thought-out layered strategy.

I don't think we ever say that we are done and it is completed and it is perfected, but I think certainly we need to continue to enhance the information we are getting. We need to continue to enhance our targeting capabilities through the automated targeting system. We need to continue with the tests that we have put in place in Honduras and also in Qasim, Pakistan and also for Southampton, meeting the requirements of the SAFE Port Act.

But also we need to make sure as far as that at some point in time we make a value determination against the risk that is present. Certainly, there are high consequences with the global maritime supply chain. Where may be some other vulnerabilities we need to focus our resources and attention as we go forward?

Ms. SANCHEZ. Thank you.

The chair will now recognize other members for questions they may wish to ask the witnesses. In accordance with our committee rules, I will recognize members who were present at the start of the hearing based on seniority on the subcommittee, alternating between the majority and the minority. Those members coming in later will be recognized in the order of their arrival.

We will go to the gentleman from Florida, Mr. Bilirakis, for 5 minutes.

Mr. BILIRAKIS. Thank you. I don't know if I am a senior member, but I will take it.

The Port of Tampa is one of the busiest. I recently spent a day with Richard here who will testify on the second panel, and he said that the greatest concern that the port has—and I discussed this with you before the hearing, Ms. Fanguy—is the TWIC card, the implementation of the TWIC card.

As you know, Florida has been a national leader, innovative, and we implemented our card called the FUPAC card in 2003. It is very similar to the TWIC card. As a matter of fact, I understand that it is interchangeable with a few exceptions.

Of course, this is a big problem for us, for the whole state of Florida, not just the Port of Tampa. I can't stress enough the importance of resolving the issues because we don't need these duplicative cards that accomplish the same purpose. It is very costly, very costly for the port and the scanner. I understand the reader is going to be very costly. I understand that the people that work at the port have to pay for the card. It is just unnecessary and inefficient.

So is there any way we can solve this problem? Have you all been working on this problem?

I would like to discuss this problem with you further. It is a big concern of people in my district and the entire state of Florida. Thank you.

Ms. FANGUY. Yes, that is a great question and very timely.

We have actually been working very closely with folks in your state of Florida to hopefully come to resolution in terms of aligning the two programs. In the past few months, we have been talking with the Department of Drug Control, the Department of Law Enforcement, and Highway and Safety in Florida to look at the two programs, specifically looking at the types of security threat assessments that the state and then the TWIC program would do to look to see where there are differences.

In the conversations that we have had, I think both sides agree that having one card is probably the right way to go, and definitely it would help to avoid redundancies for both port workers, as well as for businesses. So we are working on that and we hope to come to resolution on that soon.

In terms of the technology aspects, in the initial conversations, as you have mentioned, from a technology perspective there are similarities and we are hoping that the readers can be leveraged to actually read the TWIC cards when those are put out.

Mr. BILIRAKIS. As far as the top 10 list that they discussed earlier, I understand the July 1 deadline, and it may be extended. Is it possible that Florida can be excluded from that pilot program?

Ms. FANGUY. Do you mean in terms of that Florida would not be one of the first?

Mr. BILIRAKIS. Yes, on the TWIC card. Yes. Would you consider that?

Ms. FANGUY. We can certainly look at the deployment program, and we have been working very closely with the state of Florida to look at the overall deployment plan, taking into account some of

the aspects that they have. But again, we are trying to frontload critical ports into the overall deployment plan, so we need to look at all of those different aspects.

Mr. BILIRAKIS. I will be working with you closely. Do you envision somehow or some way in which to integrate Florida's system with the federal system?

Ms. FANGUY. The overall TWIC program in the conversations that we have had with the folks who are working on FUPAC, the conversations have been that the TWIC program would proceed. As we have discussed, there is absolutely nothing to prevent the state of Florida from doing additional checks or from having additional credentials. But again, we are hoping that from an operational perspective and technology perspective, that the TWIC card can be integrated into the existing infrastructure that exists today in Florida.

Mr. BILIRAKIS. Can you tell me the differences between the federal TWIC card and Florida's access card?

Ms. FANGUY. I would need to get back to you on the specific technology down to the bits and bytes level. They are similar, but not the same kind of card. My understanding is that the Florida card is based on similar technologies, but it is not 100 percent aligned with the federal standards that we align with.

So when we started the TWIC phase four national deployment program, we decided to align with the federal standards for credentials and biometrics. Those were on a FIPS 201. Those are the credentials that ultimately all federal government employees will have. So we are aligned with a nonproprietary standard that is put out by NIST.

Mr. BILIRAKIS. Do you feel it is possible for the TWIC card, for the Florida card to be modified to meet the TWIC standards and requirements, federal standards?

Ms. FANGUY. I am not sure if I can speak specifically to that. I think that would take some more analysis, but it is certainly possible.

Mr. BILIRAKIS. Okay, thank you very much.

Ms. SANCHEZ. Thank you. Thank you to the gentleman from Florida.

I will now call on Mr. Green from Texas for 5 minutes.

Mr. GREEN. Thank you, Madam Chair. Notwithstanding the chasm between us, it is an honor to be your ranking member today.

[Laughter.]

I thank the witnesses for providing us a great degree of jocularity today. I would also like to thank all of the many persons who have taken the time to be here. There is obviously a great amount of interest in this subject matter, and I thank you for being here as well.

I have two issues that I would like to broach briefly. The first has to do with the notion that many people are not aware that our southern border includes St. John's, St. Thomas, St. Croix and Puerto Rico. When we think "southern border," we tend to think of that area between Mexico and the United States. These islands are part of the southern border because of the ease with which persons who are on the islands can board planes and come to the continental United States.

As a result, we are obviously concerned about border security for our southernmost border, if you will. There has been an increase in traffic in the area of the waters around these borders from Cuba, from Haiti, and other places as well. And because of this increasing traffic, there has been a request made for a border patrol unit right off the Virgin Islands or on the Virgin Islands. I believe this is section 126 of the report that is due I think on May 18.

My question has to do with where are we in terms of establishing the border patrol unit, because we do have one in Puerto Rico, and I compliment our services for that one being there, but it appears that the increase in traffic may merit additional consideration.

Before you respond, let me just thank each of you public servants for the outstanding work that you do under very difficult circumstances. So would you kindly respond, the appropriate person? My suspicion is that that will be Mr. Ahern.

Mr. AHERN. I would be happy to give you some answer.

I wouldn't want to necessarily speak for Commissioner Basham or Chief of the Border Patrol David Aguilar, because it is not within my specific area of responsibility. But I do know as far as we are working diligently on the report to meet the requirement. I know you had an opportunity while you were down there, after seeing you in Honduras, the CODEL went on to the Virgin Islands and had a tour there from both the Coast Guard's and CBP's perspective.

One of the things certainly within our closest sector is over in Puerto Rico, as you point out. We are taking a look and assessing the vulnerability in that area to find out what is the appropriate deployment, and that will be in the report that we will meet the deadline on.

Mr. GREEN. Just for additional edification before I go to my next point, we met with a host of persons including the governor of one of the islands. They were all very much convinced of the necessity because of the increase in trafficking. We are talking about both human and other trafficking, drugs, smuggling, whatever. They were convinced that this is something that we should give some serious consideration to. I thank you for your answer.

The final question has to do with the TWIC card. We do have persons who are of modest means who may contend that affordability is a factor. If affordability is a factor for someone, how will we have a person who is a good worker, who wants to comply, but who literally has affordability as a factor. I am told that this card could cost as much as $137.25. If I have inaccurate information, I beg that I be corrected.

Ms. FANGUY. Your information is correct on the standard TWIC card, and there is a $32 discount if you hold a FAST card, if you are a documented merchant mariner, or if you have a hazardous materials endorsement. In terms of the overall cost of the TWIC program, we have tried to be as frugal as possible as we project out the overall costs of the program. So when we worked on the final rule, we were very careful to look at the overall cost implications of the program.

It does cost $137.25 up front, but it is a 5-year credential. So we believe that when you look at it over the 5 years, the cost over the 5 years is lower when you look at it in that way.

Mr. GREEN. Must all workers come on-line in a given sector at the same time? Or do you have a provision that will allow a person who cannot afford the cost today on a given date to have an extension of time? Is there some means by which you will try to accommodate persons who are of modest means?

Ms. FANGUY. As we roll out to the ports, as you know, we are going to be rolling out in a phased-in approach. It is in a little bit over a year period of time that we will be phasing in the program. So we will work with port stakeholders, including labor groups, to let people know where we are going ahead of time. We have informal as well as formal processes to do that, so we have government personnel who go out to the various ports ahead of time, work with port stakeholders, including labor, to let people know.

We also have advance teams from our contractor who will go out and again meet with port stakeholders, and then of course in the Federal Register, we will put out a notice announcing when we will start enrollments. But the enrollment, let me stress, is going to be over a phased period of time, so people will have an extended period of time to both get their TWIC as well as plan to get their TWIC.

Then in terms of compliance, that is actually something that the Coast Guard is going to cover, but compliance is going to be phased in based on captain of the port district. So although your port may begin enrollment during a certain time, you will have plenty of time before you have to get a TWIC, and will have notice, again, in the Federal Register, as well as informal communications through posters and working with stakeholders to let people know well in advance before compliance begins.

Mr. GREEN. I thank you very much.

Madam Chair, thank you for your generosity with the time. I yield back.

Ms. SANCHEZ. Ms. Jackson Lee, do you have any questions for our panel?

Ms. JACKSON LEE. Thank you, Madam Chair.

Ms. SANCHEZ. Five minutes.

Ms. JACKSON LEE. Admiral and others, welcome very much to what I consider to be a very important hearing. Obviously, I know that your testimony was instructive and vital, and so I may be gearing you toward questions already asked and answered.

We had a very productive delegation overview on some of the ports over the spring recess. I got a chance to see some of the challenges as well.

My question with respect to your issues goes just directly to the heart of funding resources. If we are looking back over 6 months—and I ask this question all the time—do you have everything you need for the next 6 months for this to be an effective program that is not just a review of 6 months, but now has the legs to withstand the challenges of increased tonnage, wider utilization, and certainly more utilization of your services?

Admiral BONE. I sort of answered this before, but I can say specifically with regard to the entire SAFE Port Act, I mean, I can give you areas such as integrated operations, joint operations centers, we will be building our budgets as these come on-line collec-

tively in order to establish those joint operations centers where they don't currently exist.

Other examples are, as we have already received a certain amount of resources to close vulnerabilities. As Mr. Ahern addressed earlier, we know there are other security vulnerabilities beyond containerized cargo, such as small vessels. We are working very closely collectively across DHS to close that gap and better address maritime domain awareness.

So systems and sensors that will be able to identify who is moving where and why, and the ability to intercept, as well as improved capabilities in screening technologies, and some of these Centers of Excellence that are coming forward in order to improve maritime domain awareness that Congressman Green addressed, will be built into our funding requests. Hopefully, Congress will look favorably upon those, knowing their importance, as they have in the past, in providing the additional resources for this and our improvements in spot-checks at facilities.

But I can tell you that any funding we receive will work across DHS and the other agencies, and we will be good stewards of the dollar.

Ms. JACKSON LEE. You always have. Do you need increased personnel as well?

Admiral BONE. Congresswoman, if you provide increased personnel, we will lower the risk and the threat to the public.

Ms. JACKSON LEE. You are a little stretched, and let me thank you for your service. I know that you have either been engaged in Iraq, and I know that you have been called on for many different responsibilities. We appreciate it.

Mr. Ahern, I ask the same question. I know it may be a slight redundancy, but if you forgot something and wanted to add something extra, you now have the opportunity to do so.

Mr. AHERN. Thank you very much. What I would say is basically repeat of some of the things.

Certainly, we thank the Congress for some of the resources we did receive in this year for resource to run a lot of the technology we do have in place. Our position is very similar to the Coast Guard as well. We do have a very well though out plan for deployment of technology, the appropriate resources it takes for doing that. We are in the process of formulating the appropriate budget request and working that with our department and the Office of Management and Budget.

But certainly, when you take a look at the volume and the increasing workload that we see within our legitimate travel and trade coming in, coupled with the risk that is accompanying with that legitimate travel, then the balance we have to have to make sure that we are providing the level of security that is necessary to continue to keep travel and trade growing and ensuring the economic prosperity of this country continues, we need to all the while make sure that we have the adequate strategy with the resources to execute that strategy so that we can make sure that we don't bring that travel and trade to a halt if we are not sufficiently executing the strategy and plans we have in place.

Ms. JACKSON LEE. Mr. Caldwell, you had an extensive report. If you had to pick a single issue that we needed to be reminded of or remember, what would that be out of that overview?

Mr. CALDWELL. That is a hard question. It requires a little more thought, so I could answer that for the record.

I did try to, in my opening statement, make a broad reference to the concern about resources in general. One of the other things I talked about is a push sometimes from Congress and sometimes from our other political leaders, to do things better and faster. Sometimes faster is not better, and there is a trade-off there.

But for the record, I would like to answer your question of whether I would put priority on some of the problems we have identified here. I could go on and talk for a long time, but let me just close it with that.

Ms. JACKSON LEE. Submit it in writing, and we would ask you to report back to us in writing.

Thank you very much.

Ms. SANCHEZ. I thank the witnesses for their valuable testimony and the members for their questions.

The members of the subcommittee may have additional questions for the witnesses. We will ask you to respond quickly to those in writing to the questions we may ask.

Again, I thank you for your testimony.

If I can have the second panel up, because I know some of us are trying to catch some planes. As I said, this is a traveling day for our members, and many of them end up in places where it is difficult to catch a flight after certain times. So we would like to move this along.

In order to do that, I am going to ask that you gentlemen, since we have everything in writing, to limit your testimony to 3 minutes so we get a chance to ask you questions.

I know you love me, don't you?

[Laughter.]

Anyway, I welcome you, the second panel of witnesses.

Our second panel contains four witnesses.

Our first witness will be George P. Cummings. He is the director of homeland security for the Port of Los Angeles, one of the busiest and most successful seaports in the nation. He is retired from the U.S. Coast Guard after serving 21 years as a commissioned officer.

Our second witness is Richard Wainio, the port director and CEO of Tampa Port Authority. He has a bachelor's degree from Davidson College, a master's degree from American Graduate School of International Management. He served 2 years as executive director of the Port of Palm Beach, Florida, before coming to Tampa.

Our third witness is Mr. Leal Sundet, coast committeeman, Longshore Division of the International Longshore and Warehouse Union. He has been a registered longshoreman for nearly 18 years. That is a long time.

Our last witness on this panel, Mr. Manny Aschemeyer, is the executive director of the Marine Exchange of Southern California. Captain Aschemeyer is a native of Maryland, and attended the California Maritime Academy. He has sailed extensively abroad on American-flag merchant vessels.

Welcome to all four of you gentlemen. If you will begin.

Without objection, the witnesses' full statements will be inserted in the record.

I now ask Mr. Cummings to summarize his statement for 3 minutes.

STATEMENT OF GEORGE P. CUMMINGS, DIRECTOR OF HOMELAND SECURITY, PORT OF LOS ANGELES

Mr. CUMMINGS. Thank you. Good afternoon, Chairwoman Sanchez, Ranking Member Souder and members of the subcommittee. Thank you for inviting the Port of Los Angeles to testify before you today regarding the SAFE Port Act.

You are aware, Madam Chairwoman, of the size and complexity of the Port of Los Angeles, the fact that we handle over 43 percent of the nation's cargo. There are 50 individual maritime terminals that comprise the two ports, along with complexities associated with moving other goods, petroleum, as well as a large cruise and passenger industry.

Access to the port facilities is a critical component of port security. Access control will require a comprehensive credentialing program. We consider a federal credentialing program such as the TWIC program to be a solution to this major security challenge. We fully support the TWIC program and look forward to its implementation.

Ports throughout the nation are awaiting the TWIC program full implementation to address the security challenge. The Port of Los Angeles, along with the Port of Long Beach, have been chosen by TSA to conduct the TWIC field test, which will test card-reading technologies as well as processes and procedures on the terminals before the full implementation of the credentialing and access control.

In addition to our part of the program, which will be installing the systems, the other main component of the TWIC program will be the enrollment phase. Our point on this is that it is critical that all the enrollment within the L.A.-Long Beach area is completed before we can enter the field tests. We will not be able to achieve the objectives of the field tests unless we have full enrollment of all the people within the L.A.-Long Beach. That is the longshoremen, the truckers, all the communities within the area that will require a TWIC card, are provided the opportunity to enroll before we can begin the field tests.

The enrollment team has been out to the port. They have had initial meetings with our stakeholders. However, there is much work to be done in order to achieve the milestone of full enrollment.

The Port of Los Angeles has been a participant in the Port Security Grant Program from its inception. These grant awards fund the initial capital required for us to build and develop the security infrastructure in the port for projects such as provide surveillance camera systems, a command and control center to be located in the Port of Long Beach serving the entire port complex, and a fiber-optic backbone that will connect all 50 of our maritime terminals' security systems and information systems.

We look toward this grant program to continue to fund these projects as we move forward with additional projects on the draw-

ing board for us, such as underwater and surface detection capabilities, shoreside virtual perimeter systems, and system integration of all of these security infrastructure to optimize efficiency and share data with law enforcement agencies.

U.S. Customs and Border Protection is currently operating radius and portal monitors and container imaging units in the port's container terminals. The Port of Los Angeles supports increased scanning of cargo at both ports and at foreign ports. It is critical to ensure that the movement of goods is maintained. Our concern is that CBP receive necessary resources and funding in order to achieve high levels of cargo scanning, without having a negative impact on the movement of goods.

We are also concerned on any reciprocity that may result as a result of foreign governments' reacting to steps taken by the U.S. government.

Port security training exercises are ongoing in the port complex. They are coordinated through our Area Maritime Security Committee. Each year, we have a major port security exercise which involves both industry and law enforcement agencies. We have a multitude of training opportunities that are shared for, again, both industry as well as law enforcement and agency members.

In closing, Madam Chairwoman and members of the subcommittee, we at the Port of Los Angeles thank you for your leadership in calling attention to the critical elements of port security, and one that has not been fully accomplished yet, the TWIC program in particular. We look forward to sharing the port's experience with the TWIC field test program.

Thank you again for the opportunity to participate in this hearing.

[The statement of Mr. Cummings follows:]

PREPARED STATEMENT OF GEORGE P. CUMMINGS

Good afternoon, Chairwoman Sanchez, and members of the Subcommittee. Thank you for inviting the Port of Los Angeles to testify before you today to convey the Port experiences with the implementation of the SAFE Port Act as it relates to the national Transportation Worker Identification Credential (TWIC) Program, container screenings and inspections, training and exercises, and the Port Security Grant Program.

I am George Cummings, Director of Homeland Security, for the Port of Los Angeles. I am responsible for coordination of the Port's homeland security and maritime security programs at the national, state, and local levels. As you can imagine, Port security is the top priority for the Port of Los Angeles. Not only are we responsible for the security and well-being of our tenants, workers, visitors, and the surrounding communities; but the port is also charged with maintaining the free flow of commerce that moves through our Port and that is vital to this nation's economy.

THE IMPORTANCE OF MARITIME TRADE AND SEAPORT SECURITY

As you well know, Madame Chair, the Ports of Los Angeles and Long Beach comprise the San Pedro Bay port complex through which 95 percent of all goods entering the United States arrives by container ship; and the San Pedro Bay port complex is the gateway for more than 43 percent of the containerized goods that enter the American stream of commerce annually. Together, the San Pedro Bay port complex is ranked the fifth busiest port complex in the world. Alone, the Port of Los Angeles is the eighth largest container port in the world and is the number-one container port in the United States. To further illustrate our importance to the national economy, and hence, the importance of port infrastructure security, in 2006 8.5 million twenty-foot equivalent units (TEUs) of containers entered the U.S. through the Port of Los Angeles, and 15.8 TEUs through the port complex. In addition to containerized freight, the Los Angeles/Long Beach port complex handles more than one

million cruise passengers, half a million automobiles, and more than 50 percent of California's oil.

By size, the Port of Los Angeles spans 7500 acres of real estate, including 4300 land acres and 3200 water acres along 43 miles of waterfront. The Port leases 27 marine cargo terminals with 270 berths, the World Cruise Center that hosts more than 1.2 million passengers each year, and 17 marinas that accommodate more than 3,700 recreational boat slips.

Trade through the Port of Los Angeles has grown steadily by an estimated 20 percent each year over the last five years, and we expect this trend to continue. Likewise, the industry expects national maritime trade volumes to double by the year 2020, although some economists have predicted that such doubling may occur as early as 2014 due to the demands of the American marketplace.

In the event of a catastrophic incident, whether caused by intentional acts or natural disaster, it is the responsibility of the Port of Los Angeles to stand up cargo operations as quickly as possible to minimize the impacts to the nation's economy that is dependant on trade and the movement of goods. A recent example of the affects of a major port shutdown occurred in the fall of 2002 when a labor disruption caused a 10-day shutdown of the west coast ports that brought cargo movement through the west coast ports to an immediate halt. This action cost the nation's economy an estimated $1.5 billion dollars a day (valued in 2002 dollars), disrupting the availability of goods and products that Americans rely upon daily. A healthy U.S. economy relies heavily on secure, functioning ports throughout the United States.

THE CURRENT STATUS OF THE TWIC PROGRAM

Access control at ports and port facilities is a critical component of port security, and access control will require a comprehensive credentialing program. We consider a federal credentialing program, such as TWIC, to be the solution to this major security challenge. We fully support the TWIC program and look forward to its full implementation. Ports throughout the nation are waiting for the TWIC program guidance so they may be able to fully complete their access control systems.

The Port of Los Angeles and the Port of Long Beach have been chosen by TSA to conduct the TWIC Field Test which will look at testing the card reader, processing the TWIC cards, and designing procedures at terminals for program implementation. The Field Test will also evaluate the impact of the TWIC card on the ongoing efficient movement of goods through port terminals.

In addition, the TWIC Enrollment Program is critical and must be completed before the Field Test can get underway. The TWIC enrollment team has made an initial visit to the Ports of Los Angles and Long Beach and met with port stakeholders. However, much work is yet to be done to achieve full enrollment for port and all transportation workers nationally. Full enrolment in for our port will be required before we can initiate the operational phase of the TWIC field test.

PORT SECURITY GRANTS

The Port of Los Angeles has been a participant in the Port Security Grant Program since its inception. Grant awards fund the initial capitol required to development the security infrastructure throughout the Port, and to date, funds have supported projects such as (1) a port-wide surveillance camera system, (2) a command and control center that will be located in the Port of Long Beach and serve the entire port complex, and, (3) a fiber optic backbone that will allow connectivity of all 50 terminals throughout both ports. We will look to this grant program to continue to fund critical port security projects such as enhanced surface and underwater detection capabilities, shore-side virtual perimeter systems, and system integration to optimize the efficiency of security systems and share data with other law enforcement agencies.

CONTAINER SCREENING AND INSPECTION

U.S. Customs and Border Protection (CPB) are currently operating Radiation Portal Monitors and container imaging units at all of the Port's container terminals. The Port of Los Angeles supports increased scanning of cargo, both at our port and at foreign ports where cargo is loaded. It is critical to ensure that the movement of goods is maintained. Our concern is that sufficient operational resources are made available to CBP that are adequate to support increases in cargo inspections without adversely affecting the movement of cargo. Additionally, we would want to make sure the any reciprocity requirements imposed by foreign governments for inspection of exported goods are also supported with adequate recourses so that the flow of exported goods out of the port is not adversely affected.

TRAINING AND EXCERCISES

Port security training and exercises for the Los Angeles/Long Beach port complex are coordinated through the Area Maritime Security Committee which established a subcommittee to coordinate these activities. Each year, a major port security exercises has been held in the port, and many types of security training opportunities are available throughout the year for both law enforcement agencies, emergency responders and port industry members.

IN CLOSING

In closing, Chairwoman Sanchez and members of the Subcommittee, we at the Port of Los Angeles thank you for your leadership in calling attention to the critical elements of port security, and one that has not yet been fully accomplished—the TWIC program. Also, we appreciate the opportunity to share the Port of Los Angeles's experience with the TWIC field test, and our recommendations to improve the TWIC Program. The Port is confident that the federal regulatory development process will be a speedy one, leading to the full implementation of the TWIC program, and that elements of the SAFE Port Act will be fully funded. Thank you again for the opportunity to participate in this important hearing, and I look forward to answering any questions you may have.

Ms. SANCHEZ. Thank you, Mr. Cummings.

Mr. Wainio, for 3 minutes, please.

STATEMENT OF RICHARD WAINIO, PORT DIRECTOR AND CEO, TAMPA PORT AUTHORITY

Mr. WAINIO. Thank you, and good afternoon.

The Port of Tampa is the largest of Florida's 12 active deepwater seaports, handing nearly 40 percent of the state's waterborne trade. Tamps is one of the nation's largest and most diverse seaports. Few ports in the country, in fact, face the diverse and complex security challenges that confront our port.

Florida's seaports have been at the forefront nationwide in developing comprehensive strategies for addressing security issues. At Tampa, like most ports, we rely on a very effective layered seaport security approach, working in concert with our local, state and national partners.

The Tampa Port Authority also works closely, of course, with U.S. Customs and Border Protection. At the Port of Tampa, every single in-bound container to the port is scanned for radiation through radiation portal monitors operated by CBP, without unduly disrupting port operations.

Congress is currently debating whether to require 100 percent overseas scanning of containers within 3 to 5 years, which would include both scanning for radiation and imaging. We support the effort, but we certainly urge DHS to use the pilot study approach and not to move too quickly on this because it will seriously disrupt the supply chain if it is not handled properly.

There has also been some discussion about 100 percent inspection of in-bound containers once they arrive in this country. Port directors across the country oppose this concept, which would unnecessarily and severely constrain our nation's highly efficient and effective maritime transportation system. A layered approach that includes screening or scanning of all containers as they are loaded overseas, after a pilot project is successfully tested, as well as 100 percent radiation scanning in the U.S. and 100 percent inspection by CBP of all identified high-risk containers, would significantly strengthen container security.

There has been significant enhancement of port security since 9/11 and the SAFE Port Act of 2006 should further strengthen the system. The costs, of course, as you know, have been very high.

Since September 11, Tampa Port Authority alone has committed over $50 million to security infrastructure and security personnel costs. Nearly $30 million of the total expenditures have been for security infrastructure. We have received $10.7 million from the Port Security Grant Program, so we put $20 million in out of our own pockets.

We have fared reasonably well, but we certainly advocate for the higher level of annual funding, the $400 million target that was originally set that is supported by the American Association of Port Authorities. Nationwide, the program has been sorely underfunded, and all major ports like Tampa have been forced to spend millions of dollars on projects and not funded by grants, millions of dollars that we sorely need to expand the port capacity to handle what we expect to be a doubling of business over the next 15 to 20 years.

Of greatest concern to the port community, as you have heard before, is the issue of security access credentials, the TWIC being the primary issue. There are concerns over the timetable. There are concerns over the technology. Of course, it is going to put a greater financial burden on ports and port users.

Florida's seaports have the very special concern that you have already discussed regarding access credentials. Since 9/11, Florida seaports have already successfully screened and badged over 100,000 people at Florida's ports, with 39,000 of them in Tampa alone. Federal officials and state officials have been working to resolve differences between TWIC and the Florida credentials. However, to date, there has been an apparent inability to integrate the Florida system with the federal system.

As has been repeatedly said, it will lead to duplicative security checks, separate card reader systems, with higher costs that hamper commerce without providing additional security for our seaports and our nation. I urge this committee to review the issue of duplicative criminal history checks for port access and require the development of a one-card criminal history vetting process at all U.S. seaports.

Thank you very much for this opportunity to speak with you.

[The statement of Mr. Wainio follows:]

PREPARED STATEMENT OF RICHARD A. WAINIO

Florida's 12 active deepwater seaports handle nearly 130 million tons of cargo, 4.0 million containers (TEU's) and over 14 million cruise passengers annually. The Port of Tampa is Florida's largest seaport accounting for approximately 50 million tons of cargo annually, or nearly 40% of the State's total waterborne trade.

Tampa is one of the nation's largest and most diverse seaports. The port's core bulk business includes almost 20 million tons of petroleum products—virtually all the gasoline and jet fuel consumed in West and Central Florida—and over 15 million tons of fertilizer and related products. Tampa is rapidly diversifying its cargo base into containerized freight with the recent introduction of new direct container services from Asia; shipments of vehicles and steel are increasing; and the current annual volume of 4–5 million tons of cement and aggregates is expected to double in the next few years.

Tampa is also a major cruise port handling over 900,000 cruise passengers in 2006. Additionally, the Port has the largest ship repair facilities between Pascagoula and Norfolk, and has a thriving retail / entertainment complex along its downtown waterfront area. The Port of Tampa encompasses over 5,000 sprawling acres and a relatively narrow main ship channel that stretches 42 miles across Tampa Bay. In short, few ports in the country face the diverse and complex security challenges that confront the Port of Tampa.

In Florida, the State Legislature passed security legislation (Florida Statute 311.12) prior to September 11, 2001, that mandated enhanced security standards throughout the Florida port system. The primary emphasis for the original Florida legislation was to address drug interdiction and cargo theft. This law was quickly revised after 9/11 to encompass additional requirements to prevent terrorism. With security plans in place early, Florida ports were in a position to receive and immediately implement federal security grant funds when the Port Security Grant Program began in 2002. Florida's seaports have been at the forefront nationwide in developing comprehensive strategies for addressing security issues.

Tampa has relied on a very effective layered seaport security approach. This layered approach occurs on the infrastructure side (surveillance cameras, lighting, fencing, gates, etc.) and on the personnel side, where Tampa contracts with the Hillsborough County Sheriff's Office for 24/7 coverage of all port zones within our jurisdiction. In addition, the Port Authority contracts with private security as well as employing its own professional security force.

We work in concert with our local, state and national partners. Recently, the Cooperative Vessel Traffic Service (CVTS) Tampa Bay was inaugurated. This innovative vessel traffic service allows real-time monitoring of vessels throughout the Tampa Harbor. The U.S. Coast Guard, the Tampa Bay Harbor Safety and Security Committee and the ports of Tampa, Manatee and St. Petersburg were partners in this endeavor. I commend the cooperative efforts of our community as a model for addressing and resolving security issues, and in fact, the Tampa Bay Harbor Safety and Security Committee was named the top harbor safety committee nationwide for 2005 by the U.S. Coast Guard.

The Tampa Port Authority also works closely with another of its federal partners, U.S. Customs and Border Protection (CBP). Every single inbound container to the Port of Tampa is scanned for radiation through radiation portal monitors operated by CBP. CBP has indicated that nationwide it is now scanning over 90% of all inbound containers for radiation and will increase this to nearly 100% by the end of 2008. Through careful planning, this has been accomplished without unduly disrupting port operations.

Congress is currently debating whether to require 100% overseas scanning of containers within 3–5 years which would include both scanning for radiation and imaging. The SAFE Port Act of 2006 calls on the Department of Homeland Security (DHS) to move to such a system, but first calls for a pilot program to more fully evaluate the effectiveness and practicality of this approach and required new technology. We agree with the American Association of Port Authorities that pilot projects are important and that quick implementation of 100% integrated scanning without incorporating the lessons from the pilots could be both costly and detrimental for our maritime transportation system.

There has also been some discussion about 100% inspection of inbound containers once they arrive in this country. Port directors across the country oppose this concept which would unnecessarily and severely constrain our nation's highly efficient and effective maritime transportation system. I do support the efforts to screen or scan 100% of all containers as they are loaded overseas, as well as 100% radiation scanning in the US and 100% inspection by CBP of all identified high risk containers. This layered approach would significantly strengthen container security.

The Regional Domestic Security Task Force is a unique component of security in Florida seaports that serves as the focal point for security coordination. It includes all federal and state First Responders and is headed by the local Sheriff and includes representatives of the local FBI, Florida Department of Law Enforcement and the U.S. Coast Guard. Tampa's local Area Maritime Security Committee is also very proactive and has been singled out as a national model for cooperation and collaboration.

One major annual exercise and multiple regional, state and local Port exercises are conducted within the framework of the Area Maritime Security Committee and the Regional Domestic Security Task Force. Additionally, our Hillsborough County Emergency Operations Center is a cornerstone for emergency response and coordination. Recent active Florida hurricane seasons have afforded multiple real-time opportunities to exercise the full spectrum of emergency response capabilities.

Our Regional Domestic Security Task Force brings together the leadership of the local First Responders in a very positive way. The information flow can be characterized as immediate and the leadership interacts daily. However, the flow of security information from the federal government remains bogged down due to dated security clearance requirements. A more effective security clearance system must be designed and put in place similar to the system used by the U.S. military, where an interim security clearance can be conveyed to an individual on a "need to know"

basis, allowing that individual to receive an immediate clearance to formulate a plan to mitigate an immediate threat.

There has been significant enhancement of port security since 9/11 and the SAFE Port Act of 2006 should further strengthen the system. The costs, however, have been very high and continue to increase. Since September 11, 2001, the Tampa Port Authority alone has committed over $50 million to security infrastructure and security personnel costs. Nearly $30 million of the total expenditures have been for security infrastructure. In that regard, the Port Security Grant Program has certainly been helpful. The Tampa Port Authority has received $10.7 million since the program's inception, with much of that funding going toward access control infrastructure. Tampa handles over 11,000 truck movements daily, and efficient flow of vehicles through security checkpoints is vital to maintaining and supporting the commercial base of the Port.

Though Tampa has fared reasonably well and is grateful for the federal support it has received, we do advocate for the higher level of annual funding ($400 million) supported by the American Association of Port Authorities for the nationwide grant program. Nationwide the program has been sorely under-funded with many ports unable to complete key security projects in a timely manner and all major ports, like Tampa, forced to spend millions of dollars on projects not funded by grants—millions of dollars that are badly needed for expansion of port cargo and container capacity to meet international trade demand that is projected to double over the next fifteen to twenty years years.

Of greatest concern to the port community, at this time, is the issue of security access credentials. The Transportation Worker Identification Credential (TWIC) will be another important tool to strengthen port security, but it will place an even greater financial burden on ports and port users. DHS has estimated that the card readers alone will cost $300 million. There are additional concerns over the inability to meet the timetable in the Safe Port Act in a manner that will allow for the effective and efficient implementation of the system. Also, the biometric portion of the program must be extensively tested in the maritime environment. We respectfully urge adequate staffing and funding for TSA and the Coast Guard to test and provide oversight for the implementation of the TWIC program. The biometric / technology issues with the card must be resolved prior to full scale implementation. If these issues are not resolved and significant delays occur, the commercial trade we are seeking to protect will be compromised.

Florida's seaports have a special concern and dilemma regarding access credentials. Since 9/11 Florida's seaports have already successfully screened and badged over 100,000 users at Florida's ports, to include 7 year criminal background checks on each individual. In Tampa alone about 39,000 port badges have been issued. The Florida credential, created under Florida Statute 311.12, is vetted by both the FBI and the Florida Department of Law Enforcement and is the model on which much of the TWIC is based. Federal officials and Florida officials have been working to resolve differences between the TWIC and the Florida credential. We are concerned about the apparent inability to integrate the Florida system with the Federal system which could lead to duplicative security checks, separate card reader systems and higher costs that hamper commerce without providing additional security for our seaports and the nation. A dual credential / technology system requirement in Florida will be costly, inefficient, and will negatively disrupt the progress that has been accomplished in Florida to date.

I urge this Committee to review the issue of duplicative criminal history checks for port access, and require the development of a "one-card" criminal history vetting process for all U.S. seaports.

Thank you for this opportunity to comment on these selected aspects of seaport security.

Ms. SANCHEZ. Mr. Sundet?

STATEMENT OF LEAL SUNDET, COAST COMMITTEEMAN, LONGSHORE DIVISION OF THE INTERNATIONAL LONGSHORE AND WAREHOUSE UNION

Mr. SUNDET. As you know, ILW represents longshore workers on the West Coast. We have long advocated that the ILW workforce should be utilized as the first line of defense against maritime terrorist activities, and recognized as a natural ally by law enforcement and first providers.

We are fully committed to cooperating to ensure that all West Coast longshoremen enroll in the TWIC program and are confident that all incumbent longshoremen will be deemed risk-free from a terrorist perspective.

That being the case, we must also say the credentialing will have little impact on actually securing the ports that are used as conduits. The reality is that in a modern container facility, the longshore workers has no real access to the cargo and the documentation associated with the container's contents is not readily available to the worker.

Furthermore, it makes little sense to implement a TWIC credentialing system without having card-readers in place, given that the primary purpose of TWIC is to control access to secure areas.

On the TWIC rollout itself, the challenge for the union leadership is to ensure that the membership fully cooperates. To that end, it is incumbent that enrollment centers be conveniently located so that the local union leadership will be able to ensure the greatest participation in the affected and covered workers. Charging workers a fee is counterproductive to ensuring broad cooperation. We urge the committee to reevaluate the fee and consider legislation obligating the employer to pay the fee, if our government is unwilling to appropriate funds to pay the fee.

The plan to selectively implement the actual usage of the TWIC by Coast Guard captains of port zones is potentially unworkable on the West Coast, with the exception of Hawaii. Longshoremen in Oregon, Washington and California are essential casual workers who obtain their assignments daily from a series of dispatch halls. There is an established travel system whereby workers regularly move between ports and across zones.

On the facilities security plan, refer to my written statements. On training and exercise, refer to my written statements. On pilot program and empty containers, refer to my written statements. On safety impacts of non-intrusive imaging technology, refer to my written statement.

On customs initiatives, the real threat lies in the relatively unknown content of the container, and at the various and numerous points in the transportation chain where containers can be accessed. Access to contents of containers at a modern container terminal by a rogue worker is nearly impossible. A rogue worker accessing a container would be noticed. It is an unusual event.

Yet even assuming that the shipper is a secure source, the container can be easily accessed en route to the overseas or domestic terminal. It can be accessed on the vessel. Rail operators often sidetrack containers on desolate spurs for days without security. The best use of scarce resources is in this area. Voluntary customs initiatives do not work. They need to be mandatory. The concept of pushing our borders out needs to be better financed and adequate personnel needs to be utilized in that area.

As with anything we do, there are tradeoffs. The industry has been willing to accept a higher level of risk, rather than implementing security measures that might slow commerce in any way. To principally placate the public, resources that should be used to secure the supply transportation chain outside and around the na-

tion's ports are instead used to isolate and barricade the nation's ports and their workforce. Yes, we check for radiation occasionally, and yes, we X-ray some containers. But in general, we only do so after the container has arrived and after the facility and facility workers may already have been exposed.

At the chair's pleasure, I am willing to take questions.

[The statement of Mr. Sundet follows:]

PREPARED STATEMENT OF LEAL SUNDET

Good morning Madam Chair and members of the Subcommittee:

We would like to thank you, Chairwoman Sanchez and members of the Subcommittee, for inviting the International Longshore and Warehouse Union (ILWU) to present our views on the six month status of the SAFE Port Act.

As you know, the ILWU represents longshore workers in the states of Washington, Oregon, California, Hawaii and Alaska. As a Union, we have been very active in attempting to develop and implement a system of checks and balances so as to limit the risk of terrorism activity at our work site and to keep our ports from being used as a conduit to move weapons of destruction. To that end, we have long advocated that the ILWU workforce should be utilized as the first line of defense against maritime terrorist activities, and recognized as a natural ally by law enforcement and other first responders.

In each of the states where we have presence, key union officers participate as members of the Area Maritime Security Committee. Our relationship with the Coast Guard has never been better and we applaud that agency for its cooperation with the ILWU and for performing its job admirably—often with limited resources.

The ILWU is actively participating with Lockheed Martin and its TWIC Stakeholder Communications Committee. We are fully committed to cooperating to ensure that all West Coast longshoremen enroll in the TWIC program and are confident that all incumbent longshoremen will be deemed risk free from a "terrorist" perspective.

That being the case, we must also say that such credentialing will have little impact on actually securing the ports or their use as conduits. The reality is that in a modern container facility, the longshore worker has no real access to the cargo, and the documentation associated with a container's contents is not available to the worker. TWIC credentialing is, as a practical matter, mostly a feel-good gesture promoted by those who do not completely understand modern container terminal operations as a way to diminish public and political hysteria while doing little to mitigate the real threat—container access outside of the terminal throughout the supply/transportation chain. Furthermore, it makes little sense to implement a TWIC credentialing system without having card readers in place, given that the primary purpose of TWIC is to control access to secure areas.

Given the majority support in Congress for background checks and TWIC cards after 9/11, we focused on advocating that the background check be limited to "terrorism security risks" and to ensure that there is due process for workers denied a TWIC card. However, we remain concerned that TWIC will be used to single out workers who may have a felony background but do not pose a terrorism security risk. It is imperative that waivers be granted by TSA when a worker shows no propensity to commit terrorist acts. It is also imperative that the Coast Guard have the resources and personnel to guarantee there will be sufficient numbers of Administrative Law Judges to review cases when a worker is denied a TWIC card.

Furthermore, the ILWU was approached last year by the Coast Guard to request that we help them identify our members to run their names through the terrorist watch list. We cooperated with that request and apparently they have found no matches. They apparently did not check truck drivers or many other workers with access to our ports. That process of checking longshore workers and ignoring other workers makes no sense from the standpoint of ensuring that our ports are secure.

TWIC Rollout:

In spite of the rationale for TWIC and its questionable effectiveness as a deterrent relative to security incidents, the ILWU leadership has committed its membership to cooperate. The membership knows, however, what the leadership knows. The TWIC credential is widely viewed as an unnecessary facade and in many members' views, fundamentally a privacy invasion.

The challenge for the Union leadership is to ensure that the membership fully cooperates. To that end, it is incumbent that enrollment centers be conveniently lo-

cated so that the local union leadership is able to ensure the greatest participation by the affected and covered workers.

Charging workers a fee is counterproductive to ensuring broad cooperation. We urge the Committee to reevaluate the fee and consider legislation obligating the employer to pay the fee if our government is unwilling to appropriate funds to pay the fee. In our case, attempts to negotiate with our employer group, Pacific Maritime Association to pay the fee have not been successful to date. For some workers at our nation's ports, the cost of the TWIC card is a day's pay. We would further state that the protection against terrorist activities in our nation's ports is a matter of national interest and the cost of this national security protection should be borne by the Federal government.

The plan to selectively implement the actual usage of the TWIC by the Coast Guard Captain of the Port Zone is potentially unworkable on the West Coast, with the exception of Hawaii. Longshoremen in Oregon, Washington and California are essentially casual workers who obtain their work assignments daily from a series of dispatch halls. There is an established travel system whereby workers regularly move between ports and across zones.

Facility Security Plans:

Because of the interchange of workers, West Coast terminals should have consistent procedures with respect to TWIC application and entry. In approving facility security plan modifications, the Coast Guard should do so with this in mind and not allow a given terminal to be more restrictive than the Federal rules or associated NAVIC may require.

Training and Exercises:

It has been our experience that, to date, there has been little cooperation by our employer group, Pacific Maritime Association, in utilizing the ILWU workforce as a cognitive partner in terminal awareness and reporting of unusual activity.

Anything that may have the potential for slowing commerce is ignored.

To date, longshoremen have not been trained, except where the Union has taken initiative to train its own members.

One immediate concern should have priority. The Act calls for training involving evacuation procedures and for live exercises. With some minor exceptions, the vast numbers of longshoremen have no idea, other than to run, on how to orderly evacuate facilities. Our employers resist live exercises because it may temporarily disrupt commerce and without live exercises, any plan cannot be tested and assimilated.

A second concern is that there is no plan for recovery in the event of an incident that may disable a key terminal. Given the reality, that no matter what efforts are made, it is impossible to always stop what a sophisticated "terrorist" is intent on doing, focus should be on recovery. Currently, we are in discussions with our employer group to identify cadres of longshoremen who would volunteer to specialty train and make themselves available to work in potentially hazardous environments. To ensure that this concept works, there must be cooperation to include that union leadership is integrated into emergency command structures.

Pilot Program on Empty Containers:

This very important aspect of the Act needs to be implemented. Our port facilities face a significant threat involving multiple scenarios from the domestic side. So called empty containers are a real risk as a means to transport weapons or people. Today, most terminal operators allow empty containers to pass through the gates of our ports without a visual inspection of the box to ensure that it is safe.

On March 14, 2004, ten dock workers were killed in the Israeli Port of Ashdod by suicide bombers, who were able to enter the port facilities undetected by hiding inside a cargo container. I understand that the Israelis have excellent security at their port facilities but were unable to detect people in containers being transported through their port facility. We should not have to go through a tragic event that takes our members lives before we get serious about the cargo and empty containers that enter our port through the landside.

On a related issue concerning containers, the integrity and correctness of all seals on containers must be checked as they enter a port facility and then as they are placed in inventory on the docks to detect and deter any tampering as required by regulation 33 CFR 105.265 (b)(4) and 105.265 (c)(4); presently this is simply not being done at all at most port facilities; in fact, since September 11, many facility operators have discontinued their past practice of checking seals in order to save themselves a few dollars.

Safety Impacts of Non-Intrusive Imaging Technology:

The Act requires the National Institute for Occupational Safety and Health and OSHA to evaluate the environment and safety impacts of non-intrusive imaging technology and to develop and put in place a radiation risk reduction plan to minimize the risks to workers and the public. Such evaluation needs to proceed. I am alarmed at the lack of independent study of the long-term effects of this technology on the human body. The ILWU will place the safety of our members' lives first.

Customs Initiatives:

As stated earlier, much of the focus of port security has been on ways to physically secure the terminals and scrutinize the backgrounds of port/transportation workers. While this has some marginal value, the real threat lies in the relatively unknown content of the container and at the various and numerous points in the transportation chain where containers can be accessed.

Access to the contents of a container at a modern container terminal by a rogue worker is nearly impossible. Containers are infrequently opened and done so only after approval from multiple customer levels requiring several layers of terminal management intervention. A rogue worker or group of rogue workers accessing a container would be noticed! It is an unusual event.

Yet even assuming that the shipper (foreign or domestic) is a secure source, the container can be easily accessed en route to the overseas or domestic terminal. It can be accessed on the vessel. Rail operators often sidetrack containers on desolate spurs for days without security.

> The best use of scarce resources is in this area. Voluntary Customs initiatives do not work. They need to be mandatory. The concept of "pushing our borders out" needs to be better financed and adequate personnel needs to be utilized.

As with anything that we do, there are trade offs. The industry has been willing to accept a higher level of risk rather than implementing security measures that might slow commerce in any way. To principally placate the public, resources that should be used to secure the supply/transportation chain outside and around the nation's ports are instead used to isolate and barricade the nation's ports and their workforce. Yes, we check for radiation occasionally. And yes, we x-ray some containers. But we only do so after the container has arrived and after the facility and facility workers may already have been exposed.

The members of the ILWU are proud of what they do for a living. We built the West Coast ports into a model of efficiency and competitiveness. ILWU members are patriots. They do not want anything to happen to *their* ports. They make a good living on trade and unencumbered commerce. As an institution, we have cooperated on port security since September 11, 2001 and will continue to do so even though we believe that priorities and resources have been poorly allocated and often misdirected.

Thank you for listening. We believe there were some very good aspects of the SAFE Port Act, including training and exercises, an empty container pilot program, and a radiation worker safety study. We hope that the Department of Homeland Security is prioritizing these aspects of port security. At the Chair's pleasure, I will try to answer any questions that you may have.

Ms. SANCHEZ. Thank you, Mr. Sundet.

Mr. Aschemeyer, for 3 minutes.

STATEMENT OF MANNY ASCHEMEYER, EXECUTIVE DIRECTOR, MARINE EXCHANGE OF SOUTHERN CALIFORNIA

Mr. ASCHEMEYER. Good afternoon. Thank you for inviting me here from California. I am delighted to be here.

I am here for one simple reason: to tell you that we have a system in place for long-range vessel tracking. We have been developing it now for over 5 years. We have had an MOU with the Coast Guard and have worked diligently with them to create an atmosphere of partnership with them for long-range tracking. We are hopeful that that will continue to move forward.

We believe that there is a need to enhance maritime domain awareness. We have worked diligently. I gave you a couple of graphics in your kits. I will just show you right now, this is who we are. We are located all the way around the country. We have 13 major sections of coverage. On any given day, this is our map

that we are actively—this is a real-time active picture. We can track 2,000 vessels on any given day in and out of the United States' waters from Maine to Florida, from New York to Hawaii, and up into Alaska.

This is one example I wanted to show you real quick, that we tracked a vessel from Rotterdam through the Mediterranean through the Red Sea, across the Indian Ocean, into the Far East, and then back and forth across the Pacific several times. This is real-time. This is happening now. We can do this now. You can click on any one of those dots there and you will get an immediate name of that vessel, course, speed, latitude, longitude, vessel owner, vessel operator, where it is coming from, where were its ports of call.

This, in fact, will validate the notice of arrival that the Coast Guard needs when a ship says, "I have been to those last four ports of call." Have they? We can validate that. This system does that at an eye's glance.

We are working very hard and we heard earlier about best use of taxpayer dollars. This system is available to the Coast Guard now, today. We can have it up and running. It will be virtually at no cost to the Coast Guard. That is the best use of taxpayer dollars that I can think of because it will be paid for by the industry. It will be a volunteer system. Granted, people will say, "How many are going to participate?" There will probably be those that won't, but those that won't will be the ones that you need to concentrate on.

Most ship operators are good citizens. They want to do the right thing. They want to play by the rules. If the Coast Guard comes out with a NAVIC or with a letter that says, "Look, we have a system we would like you to participate in this." This has happened up in Alaska. Virtually every ship participated—tankers, cruise ships, container vessels, tugs, barges, ferry boats, what have you. They participate when the Coast Guard said, "Would you please do this?"

So it is not an order. It is a request. It costs the shipping line operator about $3 to $4 a day per vessel to operate. We used to say it is a latte a day if you drink Starbucks. It is a very modest cost.

I know my time is very limited. I ask you to refer to my written statements. There is a wealth of information in there. I would really seriously ask you to read that in detail. If you have any questions, I would be happy to go on from there.

Thank you very much.

[The statement of Mr. Aschemeyer follows:]

PREPARED STATEMENT OF CAPTAIN MANNY SCHEMEYER

CHAIRWOMAN SANCHEZ, RANKING MEMBER SOUDER, AND DISTINGUISHED SUBCOMMITTEE MEMBERS, it is my honor to have the opportunity to appear before you today to talk about what the maritime industry is doing to enhance maritime domain awareness, and specifically with regards to long range vessel tracking. My name is Manny Aschemeyer and I am the Executive Director of the Marine Exchange of Southern California. I am here representing the Maritime Information Service of North America (MISNA). I would like to begin by giving you a brief history of MISNA.

MISNA is a national coalition of non-profit maritime information sharing service organizations that are dedicated to providing information, communications and other services in order to ensure safe, secure, efficient and environmentally sound

maritime operations. MISNA represents the commercial maritime community's shared commitment to proactively address the challenges faced by the maritime industry, as well as the U.S. Coast Guard, U.S. Customs and Border Protection (CBP), U.S. Maritime Administration (MARAD), the Office of Naval Intelligence (ONI) and other federal and state agencies in a cooperative and cost efficient manner.

MISNA membership includes maritime exchanges and associations from throughout the United States and in Canada. Maritime exchanges' operations are vital to the maritime industry and their government partners in Baltimore, British Columbia, Jacksonville, Alaska, Puget Sound, San Francisco Bay, Hawaii, Southern California, New York and New Jersey, the Delaware River and Bay, New Orleans, Virginia, Texas and Portland, Oregon. Several of the people who oversee the operations of these maritime exchanges are former Coast Guardsmen and have served as Captains of the Port at various places, and all the people who run these maritime exchanges have extensive maritime experience, including as licensed master mariners, and senior maritime industry executives.

MISNA represents a broad cross section of maritime interests in each of these regions. The work of these maritime exchanges supports vessel owners and agents, port authorities, pilots, towboat companies, stevedores and terminal operators, admiralty lawyers, customs brokers and freight forwarders, ship repair firms, employer associations, insurance agencies, marine surveyors, maritime unions (both afloat and ashore) and oil spill response organizations. Collectively, over 8,000 private and public maritime businesses, agencies and associations are represented by MISNA.

While MISNA was established as a non-profit maritime organization in 1995, several of the marine exchanges that make up MISNA have been in existence for over 125 years. Whereas the maritime exchanges in the 1800s used telescopes to spot vessels approaching the U.S. and communicated the locations of those vessels to the maritime community with messengers and semaphore, today we use state of the art technology to provide accurate and timely information on maritime operations 24 hours a day. In a sense, MISNA serves as the "eyes and ears" of the maritime community.

The maritime exchanges that make up MISNA work with every segment of the maritime and waterfront business communities, and they provide state, county and municipal law enforcement, and emergency responders with both a snapshot of river and harbor activity, detailed vessel movement and position information, detailed terminal, pier and berth data, commodity information, lightering and bunkering activity, as well as in many cases local tide, weather and current conditions. But it is our work with the local Coast Guard Sector Commands and District Operations Centers that we view as being most critical to maritime operations in the U.S. and the Department of Homeland Security and the Coast Guard's efforts to maximize maritime domain awareness.

Maritime Domain Awareness (MDA) is defined in the National Strategy for Maritime Security as being the effective understanding of anything in the maritime environment that can affect the safety, security, economy, or environment of the United States. To state it simply, MISNA is working closely with the Coast Guard and other government agencies to understand the maritime domain and what is happening within it so as to protect our ports, vessels, mariners, and the American public, as well as the supply chains that are so critical to our nation's economy. This exchange of information benefits the marine industry through increasing efficiency and minimizing delays incurred in addressing security issues.

Maritime exchanges provide their public sector partners with access to historical and anticipated vessel schedules and reports, and in many cases the Coast Guard, Customs and Border Protection and other agencies rely on maritime exchanges for access to real-time vessel position information through Automatic Identification System (AIS) displays. In addition, exchanges play leadership roles in their Area Maritime Security Committees, Harbor Safety Committees and a host of other venues where private and public maritime stakeholders convene to identify opportunities for improvement, solve problems, and address the challenges of the future.

In Southern California we are closely tied to the Coast Guard's Sector Command at Los Angeles–Long Beach Harbor, which is America's biggest and busiest intermodal cargo complex. Our Marine Exchange provides the Coast Guard with vital information 24 hours a day, 7 days a week, and 365 days a year in helping them to execute their multi-faceted mission that includes Maritime Domain Awareness, Vessel Traffic Management & Facilitation, Search-and–Rescue, Law Enforcement, Port State Control, Environmental Protection & Response, and a host of others. Similar symbiotic Coast Guard–Marine Exchange relationships exist throughout the U.S. from Maine to Alaska and Hawaii.

I would like to take this opportunity to heartily applaud the Coast Guard. Since the September 11 terrorist attacks, the Coast Guard has accepted countless new responsibilities—including their ongoing efforts to enhance maritime domain awareness, improve port security, increase vessel traffic efficiency, enforce port state controls, augment search and rescue (SAR) operations and generally make our ports and waterways safer, more efficient, and environmentally protected. I have only the greatest admiration, respect and appreciation for what they do and how they do it. Given their limited manpower, assets and funding the Coast Guard has done a remarkable job, to say the least. As Winston Churchill once said of the RAF during World War Two: "Never have so many owed so much to so few!" That same adulation can be applied to our U.S. Coast Guard today.

But maritime security is not the role of the Coast Guard alone. To the contrary, the only way to achieve maritime domain awareness to the fullest extent possible is through strong public-private partnerships. In fact, the only way to maximize maritime domain awareness quickly and in a way that is cost-effective is to utilize all existing resources. *The U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship has it right in saying that securing our maritime borders require "extensive partnerships that integrate and build unity of effort among governments, agencies, and private-sector stakeholders."*

A perfect example of public-private partnerships in action—and one that I was intimately involved in creating, and in fact appeared before Congress over ten years ago to discuss—is the Vessel Traffic Service (VTS) located at Los Angeles-Long Beach Harbor. Since 1994, the VTS at Los Angeles-Long Beach Harbor has been operated by the Marine Exchange of Southern California, in partnership with the U.S. Coast Guard. While the Coast Guard did not at first embrace the "partnership concept" we had conceived, or recognize the advantages of working in cooperation with the maritime community, the VTS has come to serve as a "national model" for other ports across the nation and around the world to study and emulate.

In February of this year the Marine Exchange of Southern California had the opportunity and distinct pleasure to give DHS Deputy Secretary Michael Jackson a first-hand look at how the Coast Guard is working in tandem with the private sector to ensure the security of maritime operations at America's busiest intermodal port facility. During his visit Deputy Secretary Jackson praised our public-private partnership and appeared genuinely impressed with our operation.

The Marine Exchange of Southern California's work to bring the VTS at Los Angeles-Long Beach Harbor online was only the beginning of MISNA's efforts to maximize the Coast Guard's ability to achieve success in its various missions. When the International Maritime Organization (IMO) mandated that all vessels be equipped with VHF-based line of sight Automatic Identification System (AIS) transponders in 2004, MISNA quickly realized that all the transponders in the world would not do anything to improve maritime operations unless there were also AIS receiving stations on shore. Using our extensive network of maritime stakeholders, MISNA quickly constructed and presently operates over 80 shore-based AIS receiving stations that range over 3,000 miles north to south from above the Arctic Circle in Alaska all the way down to Florida; and east to west over 5,000 miles from Maine to Adak, Alaska and Hawaii. While this network of AIS receiving stations is now tracking over 2,000 vessels daily in the U.S., this system is growing daily with over 100 AIS sites expected to be in operation later this year. MISNA is currently sharing much of this information with the Coast Guard.

MISNA recognized early on that AIS has serious limitations, and saw first-hand what the consequences of those limitations are, foremost among which is the limited range of AIS. AIS was originally conceived as an anti-collision "tool" for mariners to use at sea and while navigating in and out of port. AIS was not designed to provide much help in addressing maritime emergencies, especially those that occurred many miles offshore, or even just outside the proximity of an AIS receiving station. Not only does AIS have a limited range of approximately forty to fifty miles, but the information it collects and disseminates is not secure. Given these shortfalls, while still recognizing the benefits of AIS, MISNA developed the ability to track vessels around the world and destined for our ports using satellite technology.

MISNA created a Voluntary-Long Range Vessel Tracking system called the Automated Secure Vessel Tracking System (ASVTS), which combines short range (AIS) and long range (satellite) vessel tracking capabilities, and provides a way for this information to be displayed in a way that is secure but can be shared easily with stakeholders who need to analyze that data. For over five years now, MISNA has been successfully tracking vessels near our coasts and around the world. The system's unique ability to process and display both AIS and long range (satellite) data provides a means of comparing and validating vessel information, aiding the detection of anomalies and providing system redundancy. MISNA is currently tracking

tankers, cargo vessels, container ships, tugs, barges, ferries and cruise ships mostly along the U.S. West Coast and in some cases, around the world. And in Alaska, the Marine Exchange has also been monitoring Coast Guard vessels at the request of Coast Guard District 17.

After the terrorist attacks on 9/11 when the Office of Naval Intelligence (ONI) needed to improve its information gathering activities, ONI officials approached MISNA and asked us to provide information on anticipated port calls and actual arrivals of vessels. MISNA complied with that request within a few days and continues to assist the ONI in its missions, consolidating this information nationwide on a daily basis. Each year, MISNA reports to the ONI on over 65,000 thousand vessels calling on U.S. ports. We have been contracted by ONI to provide this service since December of 2001.

MISNA also entered into a Memorandum of Understanding (MOU) with the Coast Guard in 2002 and through this forum has repeatedly offered the Coast Guard assistance in attaining enhanced maritime domain awareness to aid maritime security. In many areas of the country the Coast Guard is using MISNA's AIS and long range vessel tracking information on a daily basis.

The Coast Guard consistently calls on MISNA members for long range vessel tracking capabilities. As a result, MISNA members have assisted in several high profile maritime emergencies during the past few years, some of which have been covered by CNN. In one instance, MISNA tracked the "Semester at Sea" passenger vessel Explorer when it encountered heavy seas in the Pacific and was in distress. In other instance, MISNA's tracking system aided the Coast Guard's search and rescue response to the stricken cargo vessel Selendang Ayu when it lost power and grounded in a heavy storm in Alaska. And on yet another instance, MISNA tracked the response vessels assisting the car carrier Cougar Ace when it rolled on its side in the North Pacific. While most of the vessels that utilize MISNA's long range vessel tracking capabilities do so voluntarily, MISNA was able to track these vessels without having tracked them previously, and did so in few minutes. Without MISNA's tracking capabilities, it would have taken hours to locate and track these vessels.

It is in Alaska that MISNA's AIS and long range vessel tracking capabilities are most prevalent. The ASVTS system enables the Coast Guard in District 17 to efficiently manage its resources in order to augment its search and rescue (SAR) operations, enhance maritime domain awareness, improve maritime security, promote maritime safety, better assist in waterway management, and respond more effectively to environmental emergencies. Due to concerns about the vulnerability of ships operating in the restricted and often remote waters of Alaska, Coast Guard District 17 encourages vessel operators to utilize the ASVTS vessel tracking capabilities under a voluntary, industry-funded program. The participation and compliance by the vessel owners and operators is significant with tankers, ferries, tugs, fishing boats, cruise ships and container ships being tracked as they sail to and from Alaska to other ports on the West Coast and overseas. The information provided to the Coast Guard in District 17 is used to execute search and rescue and Medical Evacuation (MEDEVAC) missions, coordinate security escorts, schedule vessel boardings, and provide data for waterways management issues on a daily basis.

Long range vessel tracking, however, is more than about just tracking ships. It is about managing risk. Effectively managing risk creates resiliency which reduces disruptions and gives the Department of Homeland Security and the Coast Guard greater control in their homeland security activities. Simply stated, you can't control something you can't see. This is why long range vessel tracking is critical to achieving maritime domain awareness.

Congress recognized the need for long range vessel tracking in 2002 when it gave the Coast Guard the authority to *"develop and implement a long-range automated vessel tracking system for all vessels in United States waters that are equipped with the Global Maritime Distress and Safety System or equivalent satellite technology" and to "use existing maritime organizations to collect and monitor tracking information under the system."* Congress reinforced this authority in the *Maritime Transportation Security Act of 2004* and in the *Maritime Transportation Security Act of 2006* before adding a date certain of April 1, 2007 in the *SAFE Port Act.* MISNA has had these capabilities the entire time, and has consistently offered to provide these capabilities to the Coast Guard in a way that would not cost them (and the American taxpayers) almost nothing.

Despite this authority, DHS has not yet maximized maritime domain awareness through tapping into the marine industry's vessel tracking capabilities. While there are ongoing efforts to correct this, these efforts will continue to fall short unless they incorporate existing and proven technologies and invest in the willingness of industry partners to work together. In other words, I firmly believe that we can do better.

While I have been focused on the security aspects of long range vessel tracking, I would like to take a moment to discuss the commercial implications of increased maritime domain awareness. While maritime domain awareness is critically important to preserving the well-being of the United States, it is only one half of this equation. Maritime domain awareness must also create an environment in which international commerce can be conducted in a safe, secure, efficient and environmentally sound manner.

The primary motivation of MISNA to develop both AIS and long range vessel tracking systems was to better serve our members. By providing more accurate vessel information, maritime exchanges support efficient maritime operations and help our members avoid or minimize fines and costly delays arising from a lack of current vessel movement information. Vessels' arrival times change continuously due to wind, fog, visibility, currents, traffic density, mechanical problems and myriad other reasons. Over the past few years, numerous U.S. and foreign vessels have been turned back to sea due to the fact that the Coast Guard did not have their actual positions or updated arrival times, costing the industry millions of dollars. This situation can be avoided by providing the Coast Guard with real time and accurate information on a vessel's entire voyage track, thereby confirming that that ship has "nothing to hide" if its ETA happens to change by a couple of hours one way or another.

To put it another way, air traffic control does not turn a plane around if it does not land at the specified time. If a plane flying from LAX to DCA has a strong tail wind that helps the plane to arrive earlier than expected, the pilots are not told to fly around in circles until its originally schedule arrival time. Neither should ocean going-vessel that do not meet their notice of arrival window, in most cases due to variable weather and sea conditions, be forced to turn around and provide an arrival update. This is especially true if they have been constantly and accurately tracked all along their voyage route by a system like ASVTS.

So what exactly does MISNA offer to the Department of Homeland Security and the Coast Guard? Simply stated MISNA offers a seamless network of maritime information sharing organizations that offer a variety of programs, services and technology designed to both improve maritime domain awareness and promote maritime commerce. The U.S. government is constantly seeking the right balance between security and trade facilitation. MISNA believes that the capabilities provided by ASVTS can help in achieving that balance.

In that vein, the National Security for Maritime Strategy, the Port Security Grant Program and various Presidential Directives have highlighted the need for enhanced information sharing as critical to targeting efforts, incident prevention and response, and improved asset utilization. In line with the Coast Guard's call for public-private collaboration in information sharing, MISNA members have suggested that the Coast Guard and other agencies work more closely together and with the maritime industry to create and use electronic information reporting systems.

DHS has made good progress in several initiatives, such as the International Trade Data System and the portal for ocean carriers to submit electronic crew manifest data to both Coast Guard and Customs and Border Protection through a single interface, but additional opportunities remain unexplored. For instance, CBP and the Coast Guard, along with various other agencies require ship operators or their agents to submit advance notice of vessel arrival and departure (NOA/D). MISNA has suggested that Coast Guard share information on notices received through the electronic NOA/D port back to maritime exchanges, similar to the way CBP will share cargo manifest data with port authorities or exchanges. This information can be integrated with and displayed as part of ASVTS, and it could improve some of the difficulties I described above with regards to trade facilitation.

There have been many questions about how MISNA's vessel tracking system compares to the Long Range Identification and Tracking (LRIT) system being developed by the International Maritime Organization (IMO) that is scheduled to be fully operational in 2009. In short, IMO's system will fall short of MISNA's system in several areas, especially in light of the fact that MISNA's system is operational today and has been proven time and again during the past five years. Here is how the two systems differ:

- The IMO system imposes limits on what information contracting governments are entitled to. The past position reports and vessels' voyage histories are not provided and information will be restricted to when the vessel first makes notification, which is typically 96 hours before arrival or approximately 2,000 miles offshore, depending on the vessel's speed. MISNA's system provides global tracking information that can reveal past history and identify prior port calls of concern and/or anomalies in a voyage.

- The IMO system will be funded by the government at a cost yet to be determined while MISNA's voluntary system is paid for by the marine industry saving the government millions of dollars every year.
- The IMO system will not share information on vessels' locations with the maritime industry. If the maritime industry does not have access to this information, how can vessel operators improve the efficiency of maritime operations with respect to safety, commerce and environmental protection?

In summary, each commercial seaport in the U.S. has a different combination of geography, governance, operating rules, ownership and mix of activities. MISNA has developed a firm grasp of this complicated picture and provides an institutional memory at each of the ports where it has a presence while providing an environment of information sharing that helps the industry to work together more effectively and enhance the activities of its government partners.

MISNA's vessel tracking, display and reporting capabilities are already significantly enhancing maritime domain awareness in a way that provides increased security and promotes efficient trade facilitation, but MISNA has the capacity to offer much more. MISNA's vessel tracking, display and reporting capabilities are supported by the maritime industry; they are cost effective; and they are ready to go right now. With these capabilities, MISNA can help the Department of Homeland Security and the Coast Guard accomplish its stated goal of *"achieving an unprecedented level of information sharing and intelligence integration."* We look forward to continuing to work with Coast Guard, CBP, MARAD, ONI and other agencies to explore opportunities designed to meet our mutual goals of improved homeland security and facilitation of commerce.

I would like to thank you, Ms. Chairwoman and Members of the Subcommittee for the opportunity to testify today on behalf of the Marine Exchange of Southern California and the Maritime Information Service of North America. I look forward to answering any questions you may have.

Ms. SANCHEZ. Thank you, Mr. Aschemeyer. We will make sure that the printouts that you have there are in the committee record.

I will now just ask a couple of questions. I know we are pressed for time, and I want to give some more time to my fellow colleagues.

Mr. Aschemeyer, why does the Marine Exchange exist? Why are you in place? Why do you already have this system in place?

Mr. ASCHEMEYER. The Marine Exchanges have been around in many cases since the 1800s. We are the respected and trusted honest brokers of maritime information on the waterfront. We are the maritime information clearinghouses. If you need to know anything about a ship—where it came from, where it is going from, who owns it, who operates it, what kind of cargo is it carrying—we are that person that does that.

But we saw a real need from a commercial viewpoint to improve port security, but also to enhance the flow of international trade. There have been instances, for example, where the NOA system, the ship misses its window by 6 hours. The ship has to turn around and is held outside of 12 miles until they sort it all out. We don't do that with airplanes. Airplanes come in, and if they get a tailwind and they are early, they don't circle them for 1 1/2 hours and say, "We can't land because you said you were going to be here 1 hour later." They let them land.

If you are tracking a vessel from point A to point B and they have nothing to hide, and you know exactly where they have been, and you know exactly what they have done, that is the kind of efficiency we are trying to achieve. But also, it would greatly enhance port security. It would greatly enhance maritime domain awareness.

Again, this system is ready to go. Now, with all due respect, the Coast Guard has done a tremendous job. As Winston Churchill

once said, "Never have so many owed so much to so few." I mean, they have really been called upon to do a lot. But by their own admission, they need partnerships to enhance what they are doing. They are trying to leverage their assets. They are trying to leverage what they do. And we are here to help them do that.

Ms. SANCHEZ. Thank you, Mr. Aschemeyer.

Mr. Sundet, you don't like the TWIC program much.

[Laughter.]

Mr. SUNDET. Well, I think that—

Ms. SANCHEZ. Why don't you think we should put it in?

In the overall aspect of it, my understanding is that when—I don't know when—but when we get this done, somebody that is up in Oakland or down in L.A. that worked yesterday in the Port of Long Beach can go up to Port Hueneme with the same card and have access onto the premises. And that this is going to be required for everybody who wants access onto the ports of California, for example, whether it is a truck driver or a longshoreman or somebody else.

Why don't you think it is going to work?

Mr. SUNDET. How much time do you have, Congresswoman?

[Laughter.]

Ms. SANCHEZ. You have about 2 minutes to answer that question.

Mr. SUNDET. Well, I am not sure it is going to work quite like that. I think that the industry is far too complicated than that. I don't see it working. But I don't want to go back and argue over so-called "spilled milk." I mean, the TWIC system is what it is and we are going to support it and try to get our people 100 percent enrolled in the process.

But I think that I agree with the previous speakers, the TSA and so forth. They need to take their time and do it right so that people aren't without work for any period of time, and that it actually works. We will see if it is going to work. I don't think that is the clear emphasis on what we are trying to do. It is easy to focus on that because that plays good to the public and the public feels good that something is being done. It is similar to an airport situation.

But the real problem is with the cargo and looking at what is inside that box, whether it is really locked, whether that seal means anything, and what has happened to it en route. And we are not spending resources on that of any significance because industry doesn't want that to happen. It is not happening.

And so if you look at it just from an airport analogy, we put this perimeter around the airplane and we check everything that is going to go onto the airplane. We check people. We check cargo. The main reason is we don't want somebody hijacking the plane, or we don't want a bomb on the plane. But what we are doing with our terminals is we are not doing that. We are bringing the cargo in and then maybe we are checking it on the out-gate. Maybe. That is a maybe. Okay?

So you take it back to the airplane situation, it is kind of like putting the bomb on an airplane, flying the airplane to its destination, and then when the airplane has landed and everybody has come off the airplane, then check them. It is kind of what we are doing.

Ms. SANCHEZ. Okay.

I just remember back to Chief Cunningham's comment about, and he used to be the chief of Los Angeles Port, when he first testified before this committee 3 years or 4 years ago now, where he said, "There are three things you need to worry about: What is in the container, what is in the box; and two, who is on the port, who is actually there; should they be there; and three, are all these different layers of different agencies and everything actually talking and working together?"

So I respectfully disagree in this instance. I think that that number two needs to be done, and I think that the TWIC, if we can get it correct, is hopefully going to make the lives of your longshoremen better.

Mr. SUNDET. I don't think that we are disagreeing, Congresswoman. I think it just has a marginal positive impact. I think that right now, there is too much focus and too much influence on getting that done yesterday, when it is a very difficult problem for all kinds of different reasons, and we are not spending even equal resources on the other end.

Ms. SANCHEZ. Oh, believe me, I am getting on the department about C–TPAT and containers initiative and all of those. We are working on them also, Mr. Sundet. Don't think we aren't.

I am going to let Mr. Souder ask his questions for however much time he may consumer, realizing he has one colleague behind him who is waiting to ask questions also.

Mr. SOUDER. I want to say I agree on the seals. That is a huge question that often gets overlooked. The bottom line is you can do pre-screening in Singapore, you can do screening on the ship, you can have screening at the place, but if the seal can be altered, you can go in at any place.

I have to go catch a plane. I am going to yield to Mr. Bilirakis. But I wanted to say this, having been a staff director, a staffer, a chairman and now a ranking member, I know it gets frustrating to our witnesses. You come in from a long way and you do 3 minutes and everything seems to go. Just know that you generated this book on our side and a similar thing on the other side. Your statement has been dissected into pieces to generate pages of questions.

There are eight people who got to comment on this, and maybe with a few more hearings, there will be 20 in America that get into this. You are in a very unique group. We appreciated each of your testimonies today because it adds to it, because it gave us a diversity to it.

Our staff, having been a staffer, we go around like ADD people, from thing to thing, but all of it mattered a lot on this and it was very helpful for us to get an overview today.

With that, I am headed to an airplane, and I am going to yield to Mr. Bilirakis.

Thank you.

Mr. BILIRAKIS. Thank you, Mr. Souder. I appreciate it.

Thank you, Madam Chairwoman, for having this committee hearing.

Ms. SANCHEZ. We will actually recognize you for 5 minutes if you would like.

Mr. BILIRAKIS. Thank you very much. I appreciate it. Thank you.

Mr. Wainio, I have a few questions. What is the Tampa Port Authority's number one port security concern, in your opinion?

Mr. WAINIO. As we have noted before, the number one concern that we have at this time is with port access credentialing. We strongly support port access credentials. I disagree slightly with my colleague here from the industry. I do think port access credentials do serve an important purpose. Keep in mind that there are two elements, basically, we are talking about. One is terrorism. The other is criminal activity.

Florida has had port access credentials in place for many years. Before 9/11, they had a law that required access credentialing, and then they came along with the FUPAC requirement as well, that they were pursuing. And now TWIC is coming down the pike. So we do believe in it. I think any industrial facility that serves as an entry point, as ports do, has to limit who goes on and off for a whole series of reasons.

We are, of course, extremely concerned over the potential for Florida ports to end up with two access cards. We think that would make security more difficult. It would not help. It would hurt security. As has been noted, it will be extremely costly for Florida, with millions of dollars in dual card readers unless they are able to do something about that. As was mentioned by a previous witness, they are working on trying to get one card reader to work. At this point, I don't think they have reached that point. It looks like if you have a FUPAC and a TWIC, you would have two separate systems, two expensive systems.

We just think that that would be extremely burdensome. It would create competitive disadvantages for ports in Florida. Take a port like Jacksonville, which is on the Georgia border competing directly with ports like Charleston and Savannah, for the container trade. They have literally thousands of truck drivers coming and going from out of state, coming into Jacksonville, and certainly will in the future when they start moving a million containers or more a year, which is coming soon at that port.

So that extra burden, that extra cost, the delays, everything involved in that duplicative effort will create significant competitive disadvantages by driving up the cost to use Florida ports. We think it is just unacceptable and we urge you, again, to insist that a solution be found to this problem.

Mr. BILIRAKIS. Thank you very much. So you are saying it is going to have a detrimental impact on commerce as well.

Mr. WAINIO. On commerce and it will not augment security in any substantial way.

Mr. BILIRAKIS. Do you have any thoughts or suggestions on how federal and state officials in Florida might resolve the discrepancies between their respective port access control credentials?

Mr. WAINIO. I am not really able to give you the answer to that. I know that in Tallahassee and, as was noted before, all of the people that are working on it—Mr. Sadler from the TSA working with Colonel Janes of the Office of Drug Control in Florida—all say we want one card. Everybody agrees we should have one card, but integrating the Florida criminal data systems with what the federal

systems are doing apparently is a hurdle at this point. They need to find a way to do that.

Our goal, again, is one card. We don't really care how they arrive at that, but I do understand that the main hurdles do have to do with the criminal background checks and the integration of the data. For example, if you violate the law in Florida—and Florida would not be unique in this case, in any state—and you have done something wrong in the state, it may not be in the FBI database. That, Florida says, is a problem.

So some steps have to be taken by the state, I assume, to find a way to provide that data to the federal authorities so they can incorporate it into the background checks that TWIC does. Again, this is not just unique to Florida. Other states apparently do not provide the data to the federal entities as well on a lot of local crimes.

Mr. BILIRAKIS. I know you touched on this in your opening statement, but could you talk about the current container security procedures in place in the Port of Tampa?

Mr. WAINIO. Yes. We are new to the container business. We just started. We built our first container terminal last year and we just started to receive ships every week direct from Asia, China, Korea, Japan, coming into our port. We expect that business to grow geometrically over the next few years, and expect to be moving hundreds of thousands of containers on an annual basis.

Our port, like most Florida ports, is ahead of the curve on security. We have had radiation portals in place for a number of years, and 100 percent of all the containers that arrive are checked. I agree with Mr. Sundet that in some cases, some could clearly argue that checking for radiation once they arrive and leave a port is a little bit late, but it is done.

We also think that Customs and Border Protection is very effective in the way that they are doing visual searches of the containers. They clearly screen the manifests. We have a new CES system—customs examination station—and they do pull all high-risk containers over to that CES and they de-van them, strip them down, and search them. So we think the security that is being accomplished related to containers at the Port of Tampa is quite good. Again, we have a small number of containers at this time.

As I indicated in my remarks, both the prepared and the oral remarks, I do believe, as I think everyone in this room probably does, that more of that screening and scanning needs to be done overseas, and that should be the primary focus on the effort.

Mr. BILIRAKIS. Is the federal funding for the security adequate, in your opinion?

Mr. WAINIO. Well, certainly nationwide, I don't believe so. I think it falls short in many areas. In the state of Florida, as I can speak directly for Tampa and Florida, over the last 5 years we have spent literally hundreds of millions of dollars on security infrastructure, most of that has come from our own pockets. We have done better than most States.

What it means is that we have had to transfer funds that would have been used for commercial projects needed to expand capacity and improve productivity. We have had to shift millions of dollars from that into security projects. Now, we need to start finding

money to do those commercial projects that have been sitting there for years undone. We do have a primary mission, and that is to move international trade. If we don't focus our resources there, we are going to start to see more and more delays and problems, and costs obviously will go up to the consumers.

Mr. BILIRAKIS. Thanks very much. I appreciate it very much. Thank you.

I yield back, Madam Chairman. Thank you.

Ms. SANCHEZ. I thank the gentleman from Florida.

Let me just ask a quick question of Mr. Sundet, and then Mr. Cummings. I would hate to have you come all the way and not get a question off of us.

Mr. Sundet, the empty containers coming from land-side, do you have any idea how many there are? How long they stay? If I should worry about these at all, when they are sitting out there in the ports?

Mr. SUNDET. I can't give you an exact number, but there are lots of them. There are lots of them.

[Laughter.]

Ms. SANCHEZ. Especially in L.A., right?

Mr. SUNDET. Especially in L.A. They stay at different intervals because they are taken onto vessels when there is room for them. Usually, they are dropping off a vessel and if they have room, they take as many empties as they can, because they need empties to bring imports back, and imports are what is moving the trade here. There is a huge imbalance between imports and exports.

We have always advocated, and we have had different ideas on how to deal with empties, but it is a very vulnerable point because too often we don't look at the domestic side of this thing, whether it be an empty container or even an export container that is coming, you know, a potential export container on the domestic side is not looked at.

I personally think that there is a significant threat of some kind of thing, you know, depending on what the scenario is that you are looking at. Say, for instance, you are going to blow up a ship in the channel, for instance, in the L.A. channel, it would be a threat. It might be easier to do that from the domestic side than it would be from the import side, or from overseas.

Ms. SANCHEZ. Thank you, Mr. Sundet.

I think Oklahoma always reminds us that sometimes we have our own born terrorists right here in the United States, and we don't look at them.

Mr. Cummings, the last question: What is the most significant security challenge that your port faces today?

Mr. CUMMINGS. I would probably refer back to what Noel Cunningham said. There are three basic areas. I think all three of them we have to continue to work aggressively. At the Port of L.A., we have to keep working on building our security infrastructure to get our ports secure, and that is the grant projects that we submit for. We get some grant money and we do engineering and contracting. We build the systems out.

I think in our estimation, between myself and my counterpart in Long Beach, we are somewhere just over the halfway line in terms of the projects that are on the drawing board. We have another set

of projects that have been identified and that need to be funded, and go through the same process of engineering and contracting.

In terms of cargo security, clearly a critical concern of ours. As you know, we move 43 percent of the nation's cargo. We see more containers than the rest of the country put together. We would advocate strongly, as my testimony included, increasing security, increasing cargo screening overseas. I mean, we really feel like if the mission and the objective is to protect the port, as has been stated across the panel here, to protect the ports you have to screen overseas.

Screening and the measures taken in the port protect the supply chain beyond us. They don't protect the port. And that has to be clear. That has to be a clear part of this discussion. There are reasons to do different parts of the security puzzle at different places, but you have to be clear on what you are accomplishing.

So cargo security done in the port of L.A.-Long Beach protects the rest of the supply chain, and that is a worthwhile mission, but it doesn't protect the port. You have to screen the cargo overseas and then you have to have a supply chain security methodology with seals and monitoring that you have some confidence in, that you have a lot of confidence in.

Ms. SANCHEZ. Excuse me.

Do you agree with that, Mr. Sundet?

Mr. SUNDET. Yes.

Ms. SANCHEZ. I am just trying to get management and labor here to agree on something.

Mr. CUMMINGS. Actually, we agree with our longshoremen all the time. We are very closely aligned in terms of port security.

Ms. SANCHEZ. I know you use them quite a bit for some information.

Mr. SUNDET. We have an excellent working relationship with the Ports of Los Angeles and Long Beach, I think.

Mr. CUMMINGS. And I guess lastly is the TWIC program. Again, as we stated, we think that it is critical. We do need to know who is on the terminals and we need to not have people on the terminals that have no business being there and that are not known people, and have had at least a check on some basic fundamentals of who they are—not an in-depth security check, not like getting a classified clearance, but some basic fundamentals.

We basically agree with the way the regulations came out in terms of what is the criteria for a TWIC card. That, we think, came out just about the right kind of checks for this level of security.

So I guess the answer is kind of all three. As Noel pointed out 3 years ago, we still have to pursue all three areas.

Ms. SANCHEZ. Thank you.

Okay, gentlemen. As my ranking member said, we really thank you for coming before us today. I know this second panel got shortchanged, but we have, will, or at least staff will read your testimony. It has been dissected. We will think about it, and of course we will probably have some follow-up questions.

The members of the subcommittee, if they have additional questions for the witnesses, we will ask you to respond quickly to those so that we can move forward.

This will not be the last time that we take a look at how the SAFE Port Act is being implemented. As I said, as a finance person, I like to continue to check and make sure what is going on. If you have any other comments that you didn't get in your testimony, please get them to our staffs and we will move forward.

Again, I thank you.

Having no further business, this subcommittee stands adjourned.

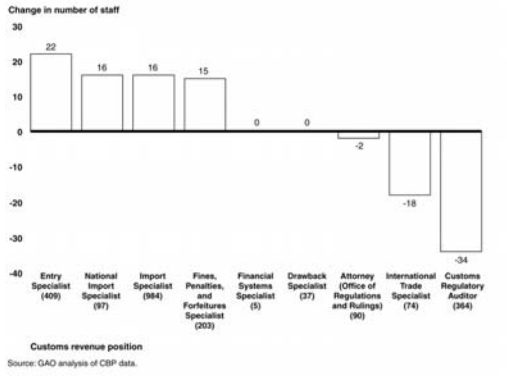
[Whereupon, at 3:07 p.m., the subcommittee was adjourned.]

VerDate Nov 24 2008 13:52 Jun 18, 2009 Jkt 000000 PO 00000 Frm 00089 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-31\48906.TXT HSEC PsN: DIANE

Appendix I: Change in Number of Staff Performing Customs Revenue Functions

This appendix provides information on the number of staff in specific customs revenue functions positions from the creation of the Department of Homeland Security (DHS) until late in 2005. The change in the number of staff in customs revenue positions and their associated support staff varies by position. Figure 3 shows the change in the number of staff in customs revenue positions; figure 4 shows the change in the number of associated support staff.

Figure 3: Change in Number of Staff in Customs Revenue Positions from March 2003 Baseline, as of December 2006

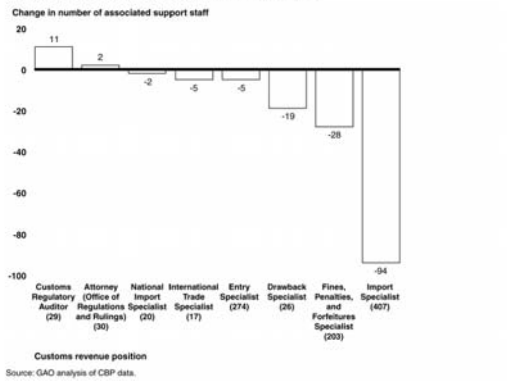


Source: GAO analysis of CBP data.

Note: Number in parentheses is the mandated baseline staff level for each position.

Note: Number in parentheses is the mandated baseline staff level for each position.

Figure 4: Change in Number of Associated Support Staff from March 2003 Baseline, by Customs Revenue Position, as of September 2006



Source: GAO analysis of CBP data.

Note: Number in parentheses is the mandated baseline staff level for each position.

Related GAO Products:

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.

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.

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

○

VerDate Nov 24 2008 13:52 Jun 18, 2009 Jkt 000000 PO 00000 Frm 00093 Fmt 6601 Sfmt 6011 H:\DOCS\110-HRGS\110-31\48906.TXT HSEC PsN: DIANE