

**TENTH ANNIVERSARY OF THE
MARITIME TRANSPORTATION SECURITY ACT:
ARE WE SAFER?**

(112-101)

HEARING
BEFORE THE
SUBCOMMITTEE ON
COAST GUARD AND MARITIME TRANSPORTATION
OF THE
COMMITTEE ON
TRANSPORTATION AND
INFRASTRUCTURE
HOUSE OF REPRESENTATIVES
ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

SEPTEMBER 11, 2012

Printed for the use of the
Committee on Transportation and Infrastructure



Available online at: <http://www.gpo.gov/fdsys/browse/committee.action?chamber=house&committee=transportation>

U.S. GOVERNMENT PRINTING OFFICE

75-850 PDF

WASHINGTON : 2012

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

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

JOHN L. MICA, Florida, *Chairman*

DON YOUNG, Alaska	NICK J. RAHALL II, West Virginia
THOMAS E. PETRI, Wisconsin	PETER A. DeFAZIO, Oregon
HOWARD COBLE, North Carolina	JERRY F. COSTELLO, Illinois
JOHN J. DUNCAN, JR., Tennessee	ELEANOR HOLMES NORTON, District of Columbia
FRANK A. LoBIONDO, New Jersey	JERROLD NADLER, New York
GARY G. MILLER, California	CORRINE BROWN, Florida
TIMOTHY V. JOHNSON, Illinois	BOB FILNER, California
SAM GRAVES, Missouri	EDDIE BERNICE JOHNSON, Texas
BILL SHUSTER, Pennsylvania	ELIJAH E. CUMMINGS, Maryland
SHELLEY MOORE CAPITO, West Virginia	LEONARD L. BOSWELL, Iowa
JEAN SCHMIDT, Ohio	TIM HOLDEN, Pennsylvania
CANDICE S. MILLER, Michigan	RICK LARSEN, Washington
DUNCAN HUNTER, California	MICHAEL E. CAPUANO, Massachusetts
ANDY HARRIS, Maryland	TIMOTHY H. BISHOP, New York
ERIC A. "RICK" CRAWFORD, Arkansas	MICHAEL H. MICHAUD, Maine
JAIME HERRERA BEUTLER, Washington	RUSS CARNAHAN, Missouri
RANDY HULTGREN, Illinois	GRACE F. NAPOLITANO, California
LOU BARLETTA, Pennsylvania	DANIEL LIPINSKI, Illinois
CHIP CRAVAACK, Minnesota	MAZIE K. HIRONO, Hawaii
BLAKE FARENTHOLD, Texas	JASON ALTMIRE, Pennsylvania
LARRY BUCSHON, Indiana	TIMOTHY J. WALZ, Minnesota
BILLY LONG, Missouri	HEATH SHULER, North Carolina
BOB GIBBS, Ohio	STEVE COHEN, Tennessee
PATRICK MEEHAN, Pennsylvania	LAURA RICHARDSON, California
RICHARD L. HANNA, New York	ALBIO SIRES, New Jersey
JEFFREY M. LANDRY, Louisiana	DONNA F. EDWARDS, Maryland
STEVE SOUTHERLAND II, Florida	
JEFF DENHAM, California	
JAMES LANKFORD, Oklahoma	
REID J. RIBBLE, Wisconsin	
CHARLES J. "CHUCK" FLEISCHMANN, Tennessee	
VACANCY	

SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION

FRANK A. LoBIONDO, New Jersey, *Chairman*

DON YOUNG, Alaska	RICK LARSEN, Washington
HOWARD COBLE, North Carolina	ELIJAH E. CUMMINGS, Maryland
ANDY HARRIS, Maryland	CORRINE BROWN, Florida
CHIP CRAVAACK, Minnesota	TIMOTHY H. BISHOP, New York
BLAKE FARENTHOLD, Texas	MAZIE K. HIRONO, Hawaii
JEFFREY M. LANDRY, Louisiana,	MICHAEL H. MICHAUD, Maine
<i>Vice Chair</i>	NICK J. RAHALL II, West Virginia
JOHN L. MICA, Florida (<i>Ex Officio</i>)	<i>(Ex Officio)</i>
VACANCY	

CONTENTS

	Page
Summary of Subject Matter	iv
TESTIMONY	
PANEL 1	
Rear Admiral Joseph A. Servidio, Assistant Commandant for Prevention Policy, United States Coast Guard	4
Stephen L. Caldwell, Director, Homeland Security and Justice, Government Accountability Office	4
PANEL 2	
Bethann Rooney, Manager of Port Security, Port Authority of New York and New Jersey, testifying on behalf of the American Association of Port Authorities	13
Christopher Koch, President and CEO, World Shipping Council	13
PREPARED STATEMENT SUBMITTED BY MEMBER OF CONGRESS	
Hon. Rick Larsen, of Washington	21
PREPARED STATEMENTS SUBMITTED BY WITNESSES	
Rear Admiral Joseph A. Servidio	23
Stephen L. Caldwell	30
Bethann Rooney	84
Christopher Koch	92
SUBMISSION FOR THE RECORD	
Rear Admiral Joseph A. Servidio, Assistant Commandant for Prevention Policy, United States Coast Guard, response to information request from Hon. Frank A. LoBiondo, a Representative in Congress from the State of New Jersey, on the availability of the Coast Guard's maritime security risk assessment model	8
ADDITION TO THE RECORD	
Passenger Vessel Association, written statement	100



U.S. House of Representatives
Committee on Transportation and Infrastructure

John L. Mica
Chairman

Washington, DC 20515

Nick J. Rahall, III
Ranking Member

James W. Cook II, Chief of Staff

James H. Zinn, District Chief of Staff

September 7, 2012

MEMORANDUM

TO: Members, Subcommittee on Coast Guard and Maritime Transportation
FROM: Staff, Subcommittee on Coast Guard and Maritime Transportation
RE: Hearing on "Tenth Anniversary of the Maritime Transportation Security Act: Are We Safer?"

PURPOSE

On September 11, 2012, at 9:30 a.m., in 2212 Rayburn House Office Building, the Subcommittee on Coast Guard and Maritime Transportation will hold a hearing to review the Coast Guard's implementation of the Maritime Transportation Security Act of 2002 (MTSA) since its passage 10 years ago and identify what improvements still need to be made to enhance the security of our nation's maritime transportation system.

BACKGROUND

The Maritime Transportation Security Act of 2002

Following the terrorist attacks of September 11, 2001, the Subcommittee developed legislation to improve the security of the nation's ports and waterways. On November 25, 2002, S. 1214, the Maritime Transportation Security Act of 2002 (P.L. 107-295) was signed into law. MTSA established a framework to improve the security of the nation's ports, waterways, and vessels from potential terrorist attacks. MTSA was codified as Chapter 701, Port Security, of title 46, United States Code.

Responsibility for carrying out the provisions of MTSA was vested in the Department of Homeland Security (DHS) and its component agencies, namely the Coast Guard, Customs and Border Patrol (CBP), and the Transportation Security Administration (TSA). On October 22, 2003, the Coast Guard issued interim final regulations (RIN1625-AA43, RIN 1625-AA46) implementing most of

MTSA's provisions. Final regulations implementing other provisions of MTSA were issued from 2004 to 2010. Final regulations governing the deployment of Transportation Worker Identification Credential (TWIC) electronic readers remain to be issued (see below).

MTSA regulates U.S. flagged vessels and domestic facilities. Foreign flagged vessels and facilities are subject to the International Maritime Organization's (IMO) International Ship and Port Facility Security Code (ISPS), which was ratified shortly after MTSA's passage. The ISPS Code was implemented to provide a standardized international framework for foreign port facilities and vessels to assess vulnerabilities and improve security. Its provisions are substantially similar to the implementing regulations of MTSA. The Coast Guard is the primary federal agency responsible for enforcing ISPS regulations on foreign flagged vessels operating in U.S. waters. Since inception of the ISPS Code in 2004, over 300 foreign vessels have been detained, expelled, or denied entry to the U.S. by the Coast Guard under the auspices of the ISPS Code.

Several subsequent acts of Congress have made amendments to MTSA, most notably the Security and Accountability For Every (SAFE) Port Act of 2006 (P.L. 109-347) and the Coast Guard Authorization Act of 2010 (P.L. 111-281). This memo will focus primarily on the Coast Guard's role in implementing the major provisions of MTSA.

Vulnerability Assessments:

MTSA requires the Secretary of Homeland Security (Secretary) to conduct security assessments of vessel types, such as tankers carrying oil or natural gas, and port facilities operating in the U.S. which pose "a high risk of being involved in a transportation security incident." The Coast Guard completed vulnerability assessments of 55 strategic port areas in January 2004. The assessments are updated every five years by the Coast Guard.

Maritime Transportation Security Plans:

In addition to the vulnerability assessments conducted by the Coast Guard, MTSA requires certain U.S. vessels and port facilities to conduct their own vulnerability assessments and develop individual security plans. These plans must: outline passenger, vehicle, and baggage screening procedures; identify an individual responsible for security; designate restricted areas within the facility or vessel; explain personnel identification procedures and access control measures; describe what equipment and infrastructure will be installed to improve security; and discuss other security procedures. The plan must be updated every five years. The Coast Guard is responsible for the review, approval, and enforcement of these security plans. There are currently 3,161 facilities and 14,533 vessels operating under Coast Guard approved security plans.

MTSA requires the Secretary to prepare a National Maritime Security Plan (NMSP) to establish terrorist incident response procedures and coordinate the duties and responsibilities of relevant federal departments and agencies. The National Strategy for Maritime Security (NSMS) and its eight supporting implementation plans released in September 2005 satisfies this requirement. Additional information on NSMS and its implementing plans may be found at: <http://georgewbush-whitehouse.archives.gov/homeland/maritime-security.html>.

MTSA also requires certain port areas to develop Area Maritime Security Plans (AMSP) which identify high risk facilities and infrastructure in the port area, establish response measures and coordinate the responsibilities of area response agencies, and identify salvage procedures to restore operations after an incident. AMSPs are developed and periodically updated by the Coast Guard Captain of the Port in consultation with members of the Area Maritime Security Committees. These committees include stakeholders from the local maritime industry, the boating public, and other relevant state and local agencies.

Transportation Security Cards:

MTSA requires the Secretary to prescribe regulations requiring individuals needing unescorted access to secure areas of certain vessels and maritime facilities to be issued a biometric identification. TSA developed the Transportation Worker Identification Credential, in consultation with the Coast Guard, to meet these requirements. The goal of the TWIC program is to develop a biometric credential that is interoperable across transportation modes and compatible with existing independent access control systems. Individuals requiring access to secure areas of MTSA regulated facilities or U.S. flagged vessels are required to obtain a TWIC. To date, over 2.1 million workers have been issued credentials.

Section 104 of the SAFE Port Act requires the Secretary to conduct a pilot program to test technology to read TWIC and its biometric identification information and established a deadline of April 13, 2009 to issue final rules for the deployment of TWIC readers. The TSA did not complete the pilot program and issue its program report until February 27, 2012. Shortly thereafter, the Coast Guard began the process of developing a Notice of Proposed Rulemaking (NPRM) for the deployment of TWIC readers. The Coast Guard now expects to publish the NPRM in the fall of 2012. The implementation of a final rule could take up to a year after the NPRM is published. A cost estimate of compliance with the reader requirement has not been prepared. Without the readers in place, TWICs are used as a flash pass as workers enter secure areas of facilities and vessels. As a result, the biometrics are not read and identities are not easily verified. However, the Coast Guard uses hand held readers to check the validity of TWICs during inspections of port facilities and U.S.-flagged vessels.

Port Security Grants:

The costs incurred by port authorities, facility operators, and state and local government agencies seeking to comply with MTSA requirements are vast. The Port Security Grant Program (PSGP), authorized under MTSA, provides matching grants to these entities to assist in the compliance with facility security plans including costs associated with security personnel, acquisition and operation of security equipment and infrastructure, and certain other security related activities. Since fiscal year 2002, over \$2 billion in PSGP funding has been made available to state, local, and private entities to improve port security. In the fiscal year 2013 budget request, the President proposes to combine PSGP and 15 other security grant programs into a single National Preparedness Grant Program.

Foreign Port Assessments:

MTSA requires the Secretary to assess the effectiveness of anti-terrorism measures in the foreign ports. In 2004, the Coast Guard established the International Port Security (IPS) program. Since the beginning of the IPS program, the Service has sent personnel to assess the security of 1,029 foreign port facilities and determine compliance with the ISPS code. The Coast Guard uses these visits to help create a threat matrix for vessels calling on U.S. ports. Vessels coming from foreign port facilities with security vulnerabilities identified under the IPS program score higher on the threat matrix and are targeted for boarding, denial of entry, or other actions upon arrival in U.S. waters. The Coast Guard currently maintains a list of 16 countries which are not maintaining effective anti-terrorism measures:

- | | |
|---|---------------------------------------|
| 1. Cambodia (except certain ports) | 9. Iran |
| 2. Cameroon (except certain ports) | 10. Liberia (except certain ports) |
| 3. Comoros | 11. Madagascar (except certain ports) |
| 4. Cuba | 12. Sao Tome and Principe |
| 5. Cote d'Ivoire | 13. Syria |
| 6. Equatorial Guinea (except certain ports) | 14. Timor-Leste |
| 7. Guinea-Bissau | 15. Venezuela |
| 8. Indonesia (except certain ports) | 16. Yemen |

Deployable, Specialized Forces:

MTSA mandates the creation of a deployable maritime security teams to enhance domestic maritime security. The Coast Guard's Maritime Safety and Security Teams (MSST) and Maritime Security Response Team (MSRT) satisfy this requirement.

Based in eleven ports nationwide, MSSTs are forces capable of rapid deployment in response to changing threat conditions and evolving maritime security needs. MSST duties include enforcing security zones, protecting military out-loads, ensuring maritime security during major marine events, augmenting shore-side security at waterfront facilities, and detecting weapons of mass destruction. In fiscal year 2011, the Coast Guard decommissioned its MSST based in Anchorage, Alaska.

The MSRT, which is based in Chesapeake, Virginia, consists of only one deployable team with a helicopter. The MSRT is a more highly specialized resource than the MSSTs and is used for more advanced counterterrorism operations. The primary duties of the MSRT are to deny terrorist acts, take security actions against non-compliant actors, perform tactical facility entry and enforcement, participate in port level counterterrorism exercises, and educate other forces on counterterrorism procedures.

Automatic Identification Systems:

Automatic Identification System (AIS) is an internationally adopted Very High Frequency (VHF)-based, short-range communication system which provides a means for vessels to electronically exchange data, including identification, position, course, and speed, with other

nearby vessels and shore-based AIS receivers. Depending on signal strength, weather, geography, and receiver capability, AIS signals can generally be received up to 50 miles away. MTSA requires certain commercial vessels operating in certain U.S. waters to carry AIS. In October 2003, the Coast Guard finalized its rule implementing the AIS carriage requirements (RIN 1625-AA67).

On December 16, 2008, the Coast Guard published a Notice of Proposed Rulemaking (NPRM) (RIN 1625-AA99) to amend the current AIS regulations to expand AIS carriage requirements to vessels operating in all U.S. navigable waters, and require AIS carriage for additional commercial vessels, including certain fishing and towing vessels. The NPRM would more than double the number of vessels currently tracked by the Service. The final rule is still under development by the Coast Guard.

Long-range Vessel Tracking System:

MTSA requires the Coast Guard to establish a long range tracking system to receive information on vessels operating beyond the scope of the existing and planned AIS system. Long Range Identification and Tracking (LRIT) is a worldwide, satellite-based automated tracking system that extends tracking capabilities up to 2000 nautical miles offshore. LRIT is a secure system in which data transmissions are made in a protected format to data centers which distribute them to countries permitted to have the information. The LRIT system provides information on vessel identity and position every six hours. It became operational on December 31, 2008. The Coast Guard collects and distributes vessel position data to participating countries in the LRIT system.

Penalties:

Individuals found in violation of MTSA or its implementing regulations are subject to civil penalties of not more than \$25,000 per day. Any vessel operated in violation of MTSA or its implementing regulations can be held liable in rem. Finally, the Coast Guard may prevent port facilities from operating and revoke or suspend the clearance of a vessel (prohibiting it from operating in U.S. waters) for violations of MTSA or its implementing regulations. Since 2004, the Coast Guard has prevented 82 facilities and 528 vessels from operating due to MTSA violations.

Recent Findings of the Government Accountability Office

Through reports and testimony before Congress over the last several years, the Government Accountability Office (GAO) has highlighted areas of MTSA implementation that are incomplete or unsatisfactory. Areas of concern include the following:

TWIC:

On May 10, 2011, the GAO released a report entitled *TWIC: Internal Control Weaknesses Need to be Corrected to Help Achieve Security Directives* (GAO-11-657). To test the effectiveness of the TWIC program, GAO reviewed program documentation, visited four

TWIC enrollment centers, and conducted covert tests at several selected U.S. ports. During covert tests of TWIC use at several selected ports, GAO investigators were successful in accessing ports using counterfeit TWICs, authentic TWICs acquired through fraudulent means, and false business cases. The Coast Guard still has not published a final rule for the deployment of TWIC readers. Without readers in place, facility operators cannot easily verify the identity of workers seeking entrance into restricted areas.

Foreign Seafarer Identification:

In a 2011 report to Congress entitled *Federal Agencies Have Taken Actions to Address Risks Posed by Seafarers, but Efforts Can Be Strengthened* (GAO 11-195), the GAO raised concerns about the ability of CBP and the Coast Guard to verify identity and immigration as a part of its onboard inspections of cargo vessels. DHS currently lacks the technology needed to conduct an onboard electronic verification, thus limiting the agencies' abilities to detect fraudulent documents while onboard a vessel.

Foreign Port Assessments:

On July 21, 2010, GAO testified before the Senate Committee on Commerce, Science, and Transportation (GAO 10-940T) and noted two hurdles facing the Coast Guard's International Port Security Program. The first was reluctance on the part of foreign port nations to allow Coast Guard officials to frequently observe their port operations. The other issue was a lack of resources to directly assist foreign ports with their efforts to enhance security measures.

WITNESSES

Rear Admiral Joseph Servidio
Assistant Commandant for Preparedness
United States Coast Guard

Mr. Stephen Caldwell
Director
Homeland Security and Justice Issues
Government Accountability Office

Ms. Beth Rooney
Manager of Port Security
Port Authority of New York & New Jersey
Testifying on behalf of:
American Association of Port Authorities

Mr. Chris Koch
President & CEO
World Shipping Council

**TENTH ANNIVERSARY OF THE MARITIME
TRANSPORTATION SECURITY ACT:
ARE WE SAFER?**

TUESDAY, SEPTEMBER 11, 2012

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COAST GUARD AND
MARITIME TRANSPORTATION,
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,
Washington, DC.

The subcommittee met, pursuant to call, at 9:30 a.m., in Room 2212, Rayburn House Office Building, Hon. Frank LoBiondo (Chairman of the subcommittee) presiding.

Mr. LOBIONDO. The subcommittee will come to order.

Today marks the 11th anniversary of that horrible day that changed America and changed the world, the terrorist attacks of September 11th. I would like to take a moment to remember those who perished on that day and those whose lives were changed forever because of it.

I also want to express our gratitude to the brave men and women working so hard both at home and overseas to improve our ability to prevent anything like that from ever happening again.

We are also approaching the 10th anniversary of the enactment of the Maritime Transportation Security Act. It was a landmark piece of legislation that established a framework to improve the security of the Nation's ports, waterways, and vessels from potential terrorist attacks.

The importance of keeping our ports and waterways secure cannot be overstated. Approximately 90 percent of all global trade and 25 percent of our gross domestic product move via the sea. A terrorist attack at any of our ports could severely disrupt the supply chain, which would be catastrophic to our fragile economy.

However, as we recognize in the MTSA, improving security at our ports and aboard our vessels means understanding how the industry operates. When MTSA imposed new security mandates on the maritime industry, it was done in a manner which did not undermine the free flow of commerce or the economic viability of the maritime sector.

I would like to praise the Coast Guard for following that critical balancing act in their efforts in implementing MTSA. Throughout the process, the Service has been fair, transparent, and relatively flexible with the large number of stakeholders in our maritime transportation system. Thanks to the leadership of the Coast Guard and the commitment from industry and their employees, I

believe our ports and waterways are much safer than they were 11 years ago.

However, although MTSA has been largely a success story, there are a couple of areas where concern remains. As has been documented in numerous hearings at both the subcommittee and full committee level, regulations governing the deployment of the Transportation Worker Identification Credential, TWIC, readers have still not been set. The Service is now telling us that it expects to publish proposed regulations sometime this fall, well over 3 years later than the original deadline for issuing a final rule.

As we continue to wait out these delays, the TWICs are no more than a flash pass. Without the readers in place, we are forcing maritime employees to pay for something that does not serve its intended purpose and we are undermining security at our Nation's ports. The administration needs to move forward on these regulations as soon as possible.

As we highlighted at our hearing in July, concerns persist with regard to implementation of requirements to improve maritime domain awareness. Specifically, the Service's inability to sufficiently tie its different MDA systems into one common operating picture as well as its somewhat duplicative approaches to tracking the same vessels have been a source of frustration. Additionally, we remain concerned that the efforts to share MDA information among stakeholders may suffer as the initiative to build physical Inter-agency Operations Centers at our ports wanes.

Finally, and more broadly, I remain worried about the Coast Guard's ability to continue to carry out their core maritime security responsibilities with an ever-increasing workload and a shrinking budget. The administration has proposed slashing the Service's budget by \$350 million and cutting the number of servicemembers by over 1,000, yet we have never asked the Service to do more than they are doing now.

Cutting funding while adding new responsibility is a formula for failure; and, unfortunately, we saw this formula playing out in the 1990s when the Coast Guard had been continually asked to do more, was given less, and then we were surprised when they couldn't meet all the mandates that were imposed by Congress. This is a very, very serious situation, and I don't believe that we in Congress can ever allow that to take place again. So we must be seriously on guard now.

Admiral, I hope you can speak to some of my concerns this morning, and I look forward to hearing from the GAO and the private-sector witnesses on some of these matters as well. I want to thank the witnesses for appearing today, and I look forward to their testimony.

Now I would like to yield to Mr. Larsen.

Mr. LARSEN. Thank you, Mr. Chairman, and thank you for convening this morning's hearing to assess the effectiveness of the Maritime Transportation Security Act, or MTSA, after 10 years of implementation. It is entirely appropriate that we evaluate MTSA today as we observe the 11th anniversary of the September 11, 2001, attacks. There can be no more sobering reminder that our work to protect our shores from terrorist threats and organizations requires our constant attention, creativity, and dedication.

I also want to acknowledge the contributions made by the U.S. Coast Guard on that day to secure New York harbor and to oversee the successful evacuation of over 300,000 people from Lower Manhattan after the collapse of the World Trade Center.

I want to thank you, Admiral. If you could pass that on to the entire Coast Guard family as well. On that day, the true definition of the Coast Guard motto, *Semper Paratus*, was made evident to all.

Mr. Chairman, border and transportation security is a pivotal function of the Federal Government in protecting the American people from terrorists and their instruments of destruction. The maritime domain is particularly daunting in scale, totaling over 95,000 miles of shoreline, 300,000 square miles of waterways, and 10,000 miles of navigable waterways. There are over 360 ports, approximately 3,100 critical facilities, and more than 14,000 vessels in the domestic fleet alone. Each one of these can present a potential target for terrorist activities, so the complexity of securing these assets is a huge responsibility.

Aside from infrastructure, over 60 million Americans are employed within 100 miles of our coasts and coastline and contribute over \$4 billion annually to the national economy.

The response of Congress to the attacks of September 11, 2001, was followed by specific targeted measures to protect the country, such as the creation of the Transportation Security Administration. It also included the passage of MTSA, which addressed the maritime domain with new requirements for passenger, crew, and cargo screening; the successful Customs-Trade Partnership Against Terrorism, or C-TPAT; and the MegaPorts Initiative that has systematically enhanced detection capabilities for special, nuclear, and other radioactive materials in containerized cargo.

Additionally, the greater use of technology to identify and track vessel movements, implementation of comprehensive biometric security measures, and the initiation of vulnerability assessments and creation of site-specific security plans were all new innovations.

The question asked today, though, is are we safer? That question is as valid now as it was in the days and weeks following the attacks of September 11th. This basic question raises some fundamental questions for which I will be interested to hear responses from our witnesses today.

Specifically, how do we know that we are in fact safer? By what metrics are we making such determinations? What are the economic effects on foreign and domestic maritime commerce and the cost to the U.S. taxpayer measured against security? I would also be interested in learning whether our witnesses believe that adequate resources are being provided to support these responsibilities.

As I mentioned during our hearing on maritime domain awareness in July, when resources were freely available to address the deficiencies in homeland security after September 11, 2001, it was fairly easy to get those dollars. But now we operate in an entirely different budget environment. Present fiscal constraints leave us little choice but to examine carefully the assets and resources we devote to maritime security, especially to the Coast Guard, whose

budget is already stretched thin over several different competing missions.

I have said before, and I will keep saying it: We cannot expect the Coast Guard to do more with less. The sad reality is the Coast Guard will be doing less with less given the current budget's trajectory. That is why we must spend effectively and wisely on those activities which provide the greatest risk reduction at the lowest cost.

Obviously, challenges remain. TWIC readers and cargo scanning requirements immediately come to mind. Yet, as our present maritime security strategies continue to evolve, we must not allow frustration over some aspects to deter other efforts. We must press on to develop a maritime security strategy that is comprehensive in scope, flexible in implementation, and adaptable to the changing tactics of those extremists who would seek to do us harm. For if there is one truth we have learned over the past 10 years, it is that terrorists and terrorist organizations will not tire in their efforts to probe, adapt, and exploit our vulnerabilities; and, like the Coast Guard, we must remain *Semper Paratus*.

Thank you, Mr. Chairman.

Mr. LOBIONDO. Thank you, Mr. Larsen.

Our first panel today we have Rear Admiral Joseph Servidio, Assistant Commandant for Prevention Policy, and Mr. Stephen Caldwell, director of the GAO's Homeland Security and Justice team.

Admiral, welcome. You are on.

TESTIMONY OF REAR ADMIRAL JOSEPH A. SERVIDIO, ASSISTANT COMMANDANT FOR PREVENTION POLICY, UNITED STATES COAST GUARD; AND STEPHEN L. CALDWELL, DIRECTOR, HOMELAND SECURITY AND JUSTICE, GOVERNMENT ACCOUNTABILITY OFFICE

Admiral SERVIDIO. Good morning, Chairman LoBiondo, Ranking Member Larsen, and distinguished members of the subcommittee. It is a pleasure to be here today to discuss the Coast Guard's role in securing our maritime infrastructure since the events of 9/11 and the subsequent passage of the Maritime Transportation Security Act.

The Coast Guard has made tremendous progress in securing America's waterways and supporting an efficient and resilient commercial environment. The men and women of the Coast Guard and the Department of Homeland Security and its components are committed to improving maritime security through continued cooperation and collaboration with State, Federal, local, international, and industry partners.

To help prevent terrorist attacks, we developed and continue to improve on an effective domestic and international maritime security regime. Our layered security strategy includes initiatives related to MTSA regulatory enforcement, identity and security processes, the international ship and port facilities security code, deployable specialized forces, and global supply chain security.

Before 9/11 we had no formal structured maritime security regimes for ports, port facilities, or ships, with the exception of cruise ships in the United States. With Congress' support and through our expansive partnerships, we now have strong and comprehen-

sive domestic and international security regimes in place. By successfully executing the requirements of MTSA and the ISPS Code, we have reduced vulnerabilities within the global maritime transportation system.

Specifically, the Coast Guard has reviewed and approved over 11,000 domestic vessel security plans and 3,100 domestic facility security plans, overseen the development of 43 port-specific area maritime security plans and committees, completed port security assessments for all U.S. ports using the maritime security risk analysis model while collaborating with local officials and stakeholders, visited almost 160 foreign countries to assess the effectiveness of their port security measures and ISPS Code implementation, and overseen the continued development of the National Maritime Security Plan which supports the National Strategy for Maritime Security.

Implementation of MTSA requirements such as mandatory access control measures, designated restricted areas, and screening protocols for persons and vehicles entering facilities have hardened physical security in our ports. Our continued work with TSA to implement the biometrically enabled Transportation Worker Identification Credential is an important part of this effort, and we are biometrically verifying almost 100 TWICs daily at facilities and on vessels. We work closely with Customs and Border Protection to identify and evaluate cargo risks before arrival and, when necessary, control vessels and cargo that may pose a threat.

Finally, response and recovery protocols established and exercised with Federal, State, local, and industry partners build a resilient maritime community, one able to recover more quickly from any disruption.

In closing, I was the captain of the port in San Juan, Puerto Rico, on September 11, 2001, and my brother Larry was working at the Number Three World Financial Center, a building seriously damaged in the terrorist attacks. I did not know he survived the attack and lost many friends until late that night. I was transferred from San Juan to Coast Guard headquarters, and I served on the team responsible for implementing MTSA and the ISPS Code. I am deeply committed to protecting our Nation and our people, and I know firsthand how far we have come since MTSA was passed.

I look forward to continuing to work with Congress in enhancing maritime security and providing oversight. I thank you for the opportunity to testify today, and I am happy to answer any questions you may have.

Mr. LOBIONDO. Thank you, Admiral.

Mr. Caldwell.

Mr. CALDWELL. Chairman LoBiondo, Ranking Member Larsen, and Mr. Cummings, good to see you today and thank you for inviting GAO to testify on MTSA as we approach the 10th anniversary of this landmark legislation.

My written statement summarizes almost 10 years of GAO work evaluating programs to provide for maritime security, and in our statement we include a detailed appendix on some of the individual programs with information on what the programs were designed to

do, what GAO found and recommended, and what those programs cost where we were able to find cost information.

As noted by Admiral Servidio, Federal agencies, particularly DHS and its components, have made substantial progress in implementing maritime security programs such as MTSA.

Agencies have developed or facilitated the development of security plans at the national, port, facility, and vessel level.

Agencies have screened inbound foreign-flagged vessels as well as foreign seafarers to ensure compliance with security regulations.

Agencies have enhanced their awareness of the maritime domain through extensive risk assessments with MSRAM, through vessel tracking, and for information sharing through both formal and informal means.

Agencies developed partnerships to get advanced information on incoming cargo to identify the highest risk cargo and to ensure that, as appropriate, it was screened or scanned at domestic or overseas ports.

DHS encountered many challenges along the way in implementing these programs. Many of these challenges have hindered or delayed MTSA. There has already been some discussion of that. At the high level, some programs had a lack of planning, weak program management, and lax implementation. Some programs also experienced a lack of or difficulties in coordinating with a multitude of maritime stakeholders.

As Mr. Larsen discussed, there were also limits on the level of resources available to start, operate, and sustain many of these programs; and today's more austere budget requirements has exacerbated many of these resource challenges.

Finally, there have been and still are difficulties measuring the results of the security programs.

Because of these problems, there is still some unfinished business in implementing MTSA. Chairman LoBiondo has already talked about TWIC. I will talk about three other examples.

Soon after 9/11, Interagency Operations Centers showed great promise in Charleston, Norfolk, and San Diego. Congress mandated that DHS replicate such centers at all high-risk ports. But the efforts have been plagued by limited and irregular funding, delays in developing detailed requirements, a lack of input from some of the key stakeholders, and weak management of the acquisition. It remains an open question whether the still-planned IOCs will be more than just single-agency command centers or the "Interagency" Operations Centers that Congress had intended.

The Port Security Grant Program was another program enacted soon after 9/11 with good intentions to provide funding for security improvements. While these monies have been distributed, the program has suffered from a number of problems. Program management has moved among several different agencies over the years which has reduced long-term accountability; the procedure for awarding and distributing funds was complex and slow, leading to a large accumulation of unspent funds; and, finally, despite assurances since our 2005 recommendation that the program would develop performance measures, there has been little progress determining what the \$2 billion program has actually bought.

Several different container security and scanning technologies were pursued with high hopes that they would allow us to sufficiently scan every container bound for the United States. But some premature efforts to move from research and development directly into full deployment of new technologies as well as several unsuccessful pilots at foreign ports have shown we clearly have to re-evaluate what we can actually do within the existing technical, logistical, economic, and diplomatic realities of the container-based international supply chain.

I would like to end on a positive note and acknowledge there has been substantial progress in that, collectively, these programs have improved the security of our ports. GAO will continue to evaluate a number of maritime security programs for this committee and others in Congress with the common goal of ensuring that ports remain safe and efficient engines for economic prosperity.

I would be happy to respond to any questions now.

Mr. LOBIONDO. Thank you, Mr. Caldwell.

Admiral, the President's fiscal year 2013 budget would cut funding for the Coast Guard by nearly \$350 million and over 1,000 service men and women. Talk to us about what you see these proposed cuts meaning, their impact. What does it mean to the Service's ability to conduct port security? How does it impact traditional missions? I am very concerned about this. I would like to hear your take on it.

Admiral SERVIDIO. Chairman, with increasing responsibilities and a declining budget, we will be challenged to continue all that we are doing. As Ranking Member Larsen said, we are going to have to look at risk-based decisions. We are going to have to look at how we best address those risks and focus our resources on those activities we are performing that have the greatest impact.

We do continue to use various metrics and tools, such as MSRAM, to look at the risks that we have and to drive those risks down; and once we have seen that, we can devote resources to other areas. But, as you highlighted, sir, it will be a challenge to continue to do more if the budget is less.

Mr. LOBIONDO. The Coast Guard's authorization act of 2010 required the Coast Guard to make their maritime security risk assessment model available in an unclassified version to facility and vessel owners to assist in the development of their risk assessments. The deadline on the Service to do this was 180 days. Why has the Coast Guard not met this legal requirement?

Admiral SERVIDIO. Mr. Chairman, I was unaware of that, but I can speak firsthand when I was captain of the port in St. Petersburg, Florida, all of the maritime industry—the stakeholders, the members of the Area Maritime Security Committee, and likewise the members of the Harbor Safety Committee—knew what was the factors in MSRAM. They were active parts in our development of the MSRAM each and every year and the revalidation of where we saw the risks are and what our action plans were to reduce those risks.

Likewise, we shared the MSRAM data with the Urban Area Security Initiative, the Florida Regional Domestic Security Task Force, and other law enforcement agencies so that together in the port complex we could see what the greatest risks are and how we

could utilize all of our different funding sources and our resources and our authorities to drive down those risks.

Mr. LOBIONDO. I am not sure that that is an answer to the question. Maybe you need to try to get back to us.

Admiral SERVIDIO. I will get back to you, sir, on the specifics of that.

[The information follows:]

This requirement has been met by the Coast Guard. In November 2011, the U.S. Coast Guard released a non-classified version of the Maritime Security Risk Analysis Model (MSRAM) titled the Industry Risk Analysis Model (IRAM). IRAM is a terrorism risk analysis tool that employs a similar scenario-based construct as MSRAM and calculates a relative risk index number for scenarios based on threat, consequence, and vulnerability factors. The data for each factor is entered by the owner-operator of the regulated facility or vessel and then IRAM calculates the risk index number, which can be sorted to identify high-risk scenarios. IRAM allows owner-operators to perform a terrorism-focused, security risk analysis of their facilities/vessels, provides a risk-based planning capability for updating operations plans, and provides a means to communicate risk information between owner-operators and first responders. To date, six owner-operators have requested and been provided the IRAM tool.

Mr. LOBIONDO. Moving to TWIC, can you tell us when the final rules on the use of TWIC biometric readers and the implementation of Section 809 of the Coast Guard Authorization Act of 2010 will be published?

Admiral SERVIDIO. Sir, it has the Department's highest priority, and it is presently in internal clearance.

Mr. LOBIONDO. Well, Admiral, I guess I am expecting you sort of had to say that, but it is almost laughable. It has had the Department's highest priority for years; and if that is the highest priority and how they are dealing with it, I do know the frustration that we share here of how poorly this has been managed. We just can't get answers out of them, and I guess I was hoping beyond hope there would be a little bit more specifics about this.

It is beyond frustrating. We have got a law that is in place. It has been ignored. It has been passed over. Congress—it is almost as if we are not asking questions, and the Department just doesn't seem to care about this.

And I don't put all this blame on the Coast Guard. You are forced to react to what the boss says. But I don't know whether maybe we should go on a tantrum and a tirade and Rick Larsen and I figure out how to pound our shoe on the table together or something.

Mr. LARSEN. You don't want shoes off.

Mr. LOBIONDO. We don't want shoes off. OK. We will figure out something else. Because I think I speak for everybody on the committee, this is a high level of frustration here.

Admiral SERVIDIO. Mr. Chairman, sir, with regards to 809, we did put a policy in place in December of 2011; and over 500 merchant mariners have been able to receive merchant mariner credentials without having a TWIC. That is about 250 or more received it just the last month. So we are doing what we can from a policy standpoint, sir.

Mr. LOBIONDO. OK. Mr. Caldwell, since enactment of MTSA, has the Department of Homeland Security, the Coast Guard or Customs developed any metrics or performance measures to determine the effectiveness of their efforts to secure the Nation's ports and waterways?

Mr. CALDWELL. There have been a couple of performance measures put in place. MSRAM is probably the most positive one at an individual facility level. MSRAM has been mentioned by Admiral Servidio. And we have done a recent report on MSRAM. It was very positive, and MSRAM is probably one of the better risk management tools in the Department.

Measuring the larger issue of security at the port level, this has been a tougher issue. The Coast Guard developed a metric to look at the percentage of risk that its activities have reduced in the maritime domain and in ports. Last year when we looked at MSRAM we also looked at this metric. We thought methodologically the measure was adequate, but it overstates the accuracy since it is really based on judgment of a lot of Coast Guard experts. So to say they have reduced exactly 85 percent or 30 percent of the risk was perhaps overstating the case. Coast Guard has agreed to keep using that measure but to use it at a reduced level. But that metric has probably one of the more serious attempts to look at it portwide.

As far as CPB, most of the metrics have been at the individual program level, and those metrics have generally measured their activities as opposed to measuring the results in terms of reductions in actual risk. As you know, it is hard to measure security, particularly deterrence, which is probably one of the positive accomplishments of a lot of these programs that we have now.

Mr. LOBIONDO. The SAFE Port Act of 2006 set a deadline of not later than April 2009, for the issuance of final regulations governing the deployment of technology at ports and aboard vessels to read TWICs. Now, more than 2 years later, there are still no TWIC readers. Until the readers are in place, can you give us any level of assurance that TWICs are providing adequate access, control, or improved security at our ports?

Mr. CALDWELL. TWIC acts as a fast pass right now. We did some work last year which showed that it is relatively easy for our investigators to use fraudulent TWICs or to obtain them fraudulently and then use them to get into secure facilities. We have work right now that is looking at the pilots in detail which will shed light soon on where DHS is in terms of actually using TWICs as biometric identification, as was originally intended.

Mr. LOBIONDO. Thank you.

Mr. Larsen.

Mr. LARSEN. Admiral, thanks again for coming and helping us out this morning.

With regards to container screening in the SAFE Port Act, we required 100 percent screening of containers entering the U.S. earlier this year, but Secretary Napolitano deferred meeting this requirement until 2014.

In your opinion—if the Coast Guard has an opinion on this issue—can this be done in an economical and cost-effective manner and is the problem less with technology and more with increased cost to shippers and delays and disruptions to the flow of commerce? What are the hurdles to achieving 100 percent screening?

Admiral SERVIDIO. Ranking Member, I don't think I am in a position to best answer that question. I can say that we work with Customs and Border Protection to screen every person, every vessel, and all of the cargo that comes into the U.S. We do that electronically. We do that looking at the history, using a number of different tools. That is what we are doing at present. But I am really not in a position to comment on physically inspecting all of the containers, sir.

Mr. LARSEN. With regards to performance measures—I am not going to ask you to talk percentages or so on—but it strikes me everything we have asked the Coast Guard and many other agencies to do—and this is going back to 2002, which is a long time for me to think back—still, how much of that in any way, shape, or form were we doing before we passed MTSA, to give an idea of the advances that we have made?

Admiral SERVIDIO. Sir, I had no tool that could calculate what the risks were in the various—I had 21 commercial ports when I was down in San Juan, including the largest oil terminal and the largest cruise ship port in the U.S., and we really had no measures of seeing what those vulnerabilities were and we had no systematic way of reviewing them or addressing what those risks were.

I think MSRAM is an important tool in looking at a metric on how we are reducing risk. We see that at the port level each year when we revalidate it. We can determine how the risks have been reduced.

Likewise, we have seen detention rates for security violations each year going down, the number of vessels we are detaining for security requirements are also going down, and the number of facilities we need to take control actions on are likewise going down each year.

Mr. LARSEN. And going down because of—

Admiral SERVIDIO. Because of MTSA, because of the training that we have done, because of the exercises we have done, because of the socialization, the fact that security is now part of what is expected in the maritime environment and it is part of our day-to-day operations, sir.

Mr. LARSEN. And we didn't see that nearly as much pre-2001?

Admiral SERVIDIO. No, sir.

Firsthand, other than cruise ships, we had very little security. I know in Florida at the time, in 2000, they were talking about actions to be taken to reduce theft, pilferage, other types of things at the maritime—in the maritime environment and facilities. And as a result of MTSA, those discussions are no longer going on.

Mr. LARSEN. With regards to ISPS screening, you noted the Coast Guard has visited almost 160 foreign countries to assess the

effectiveness of port security measures and implementation of ISPS Code requirements. Can you shed some light on that process a little further for us?

Admiral SERVIDIO. Yes, Ranking Member. At present, it is approximately every 2 years we look to visit foreign countries to ascertain their implementation of the ISPS Code, what they are physically doing, and it is also to establish a relationship.

For example, just yesterday, we had representatives from Djibouti, Kenya, and Somalia that were part of a reciprocal visit. We visited their countries, except for Somalia. At the present time, due to security reasons, we aren't sending anyone to their country. But we visited their countries, and they come here, and we go over our program. We highlight what we are doing, how we are doing it. And it is this exchange of both information, of training, that we feel has substantially increased the security level.

What we do is we ensure that the countries are fully implementing the ISPS Code. If they are not, it goes through an inter-agency process, sir; and if it is determined that the country has not effectively implemented it, there are conditions of entry that are required for vessels that have called on that country in the last five port calls. We could potentially delay the vessel's arrival, verify security precautions, screen them, or do a number of other control actions before that vessel actually enters the U.S.

Mr. LARSEN. And you are meeting with port representatives? Because some of these countries either have much weaker Coast Guards or no Coast Guard.

Admiral SERVIDIO. Yes, sir. Yesterday was the commandant of the Djibouti Coast Guard. It was their port facility leader for Kenya. It was their minister responsible for port security. And for Somalia it was one of their port managers that was visiting with us.

Mr. LARSEN. Thank you.

Mr. Caldwell, with regards to MSRAM, considering the Coast Guard depends upon MSRAM, we have heard what an important tool it is in its risk-based security framework, if Coast Guard officials are saying now—and they are saying—that personnel cuts are limiting the use of MSRAM data, what are the implications if the Coast Guard's budget were to continue to be cut? It is one thing to have a great tool to use. It is another thing not to be able to use it.

Mr. CALDWELL. Well, in a recent report on MSRAM we did have some concerns about whether Coast Guard field staff who worked on MSRAM at the sectors had the time to use the tool accurately and to update the data in it. One of the strengths of MSRAM that we found at the Coast Guard is that on an annual basis they are revalidating the data. So it wasn't just a one-time entry process.

Mr. LARSEN. And the Admiral mentioned that.

Mr. CALDWELL. In terms of the training.

The biggest concern we have with MSRAM is not as much in the analysis. It is to what extent is it actually useful for making decisions at an operational level. For example, MSRAM can tell you the risk at a facility and what you might do to reduce vulnerabilities at a facility. What is harder is for that captain of the port to then make decisions of how to use that risk information from MSRAM.

Because, of course, the captain of the port has 10 other statutory missions to engage. So while MSRAM might indicate it is a good idea to escort this cruise ship or this tanker that is coming into port, the captain of the port, he or she may have a search and rescue case going on or some military out-load to escort or other things, other priorities. But there will obviously be a little less fidelity in the model if we reduce the resources dedicated to keep it current.

Mr. LARSEN. Well, if you are following the Coast Guard on Twitter like I do, you will note that they are pretty busy all over the country every day doing a lot of things that probably don't have anything to do with MSRAM, including up in the Northwest. So we have to do a better job ourselves up there.

Mr. Caldwell, you have written—I noted in your written statement about the WatchKeeper Program. This new information management and sharing system has been dogged since its inception due to the lack of good engagement between the Federal, State, and local agencies and port partners with the Coast Guard in developing the requirements. Furthermore, you assert the situation has had a negative impact on the formation of these IOCs.

At this point, is it possible for the Coast Guard to reconfigure WatchKeeper or better engage partner agencies and stakeholders to provide the type of information that was first envisioned under MTSA when it was passed from an outside GAO point of view?

Mr. CALDWELL. If you think of these centers and what they were intended to be originally, I don't think they are going to be "centers" at all. They are not going to be a physical place where people actually gather. Given the costs associated with building those physical centers, the next best thing is to move to a virtual model where you could share information via WatchKeeper.

The beauty of the physical centers is that every agency could bring in their own IT tools and have it there, and it might not be all systems on one screen, but they all have their equipment there and can share information by looking at things and look at their own systems.

With WatchKeeper, there is some way to salvage it, but it will require a lot of attention, and the Coast Guard has not requested funds beyond 2013 to continue implementing that. It would take a pretty strong outreach effort. We found that 82 percent of the stakeholders that were given access to WatchKeeper had never even logged on. So the Coast Guard has a long way to go to fix that.

It is the outreach piece they are going to have to work on. Even the Federal agencies are not participating.

Mr. LARSEN. Admiral, do you have comments both on WatchKeeper and on the brick and mortar IOC versus the virtual IOC issue?

Admiral SERVIDIO. Ranking Member, I recognize there are going to be some challenges in getting ports to fully utilize WatchKeeper, because over the last 10 years there has been other systems that have been developed for some of that internal communications.

Going back to when I was in St. Petersburg, we had a joint teleconference every morning with Customs and Border Protection, with the local sheriffs, with the Tampa Police Department, where

we would go over who is going to be patrolling in what areas, what the risks were, what high-risk activities were taking place, who would be providing patrols and escorts and other types of things.

Translating some of that into WatchKeeper now that that system has been rolled out, it is going to take some change in people's attitudes. And in most of our ports likewise there have been other systems that we have used. But I think as WatchKeeper goes to 20 different ports by the end of this fiscal year we will see that it is going to be a tool that will be used more in the ports. But, right now, I think there are other tools and communication structures that some people are using. So we are going to have to build to it, sir.

Mr. LARSEN. All right. Thank you.

Thank you, Mr. Chairman.

Mr. LOBIONDO. All right. I would like to thank you, Admiral. Thank you, Mr. Caldwell. We will take a brief break while we reconfigure for the second panel.

OK. We will reconvene. The second panel this morning is Ms. Bethann Rooney, manager of port security of the Port Authority of New York and New Jersey, who is testifying on behalf of the American Association of Port Authorities.

We also have Mr. Chris Koch, who is president and CEO of the World Shipping Council.

Both Mr. Koch and Ms. Rooney were tremendously—very, very, very helpful to this subcommittee as we went about our business and the process of drafting MTSA 10 years ago and trying to get it right and understand how it works in the real world. So I want to thank you for your help then and thank you for being here today.

Ms. Rooney, you are recognized.

TESTIMONY OF BETHANN ROONEY, MANAGER OF PORT SECURITY, PORT AUTHORITY OF NEW YORK AND NEW JERSEY, TESTIFYING ON BEHALF OF THE AMERICAN ASSOCIATION OF PORT AUTHORITIES; AND CHRISTOPHER KOCH, PRESIDENT AND CEO, WORLD SHIPPING COUNCIL

Ms. ROONEY. Good morning Chairman LoBiondo, Ranking Member Larsen, subcommittee members. Thank you for inviting us here today to discuss MTSA over the past decade.

Prior to 9/11, security was not a top concern for most U.S. ports. Eleven years ago today, that all changed. Congress and the administration took quick and decisive action to focus on the risk to our seaports. Enhancing maritime security and protecting our ports from acts of terrorism and other crime remains a top priority for the American Association of Port Authorities and our members. Protecting America's ports is critical to our Nation's economic growth and vitality and is an integral part of homeland security and national defense.

The challenge for the past 10 years, however, has been to integrate security into the efficient and economic flow of commerce. We commend the Coast Guard for its excellent job in developing the regulations and working in partnership with industry to secure our ports.

Maritime security is a continuous activity that requires the attention of many individuals. The cost of meeting and maintaining the requirements of the security regulations is significant. Implementing MTSA is not a one-time expense. Rather, it requires recurring costs to operate, maintain, and staff the equipment and systems that were put in place. My agency alone has spent \$166 million on port security in the past 11 years.

As was mentioned, the foundation of a good security program is a risk assessment tool. MSRAM should be used by all Federal agencies to assess the risks in the maritime environment, and, as has also been mentioned, we would like to see MSRAM made available to regulated entities to assess the risk of their own facilities.

Key to enhancing and maintaining security in ports is the Port Security Grant Program. Our economy, safety, and national defense depend largely on how well we can protect our seaports, and cuts in Federal funding present significant challenges to the security of our ports. We urge Congress to provide full funding for the Port Security Grant Program.

DHS is proposing to merge all grant programs into a single program that would be managed by the States. We encourage your committee's continued support to voice opposition to this new structure.

The Port Security Grant Program is one of just a few security grants that requires a cost-share. At a minimum, we urge Congress to direct the Department to eliminate the cost-share for public agencies and our tenants. We also ask for this committee's assistance to ensure that the performance period for port security grants is no less than 3 years.

While the MTSA authorized grant funding to be used for equipment that detects weapons of mass destruction and conventional explosives, grant funding cannot be used to fund Federal functions such as cargo inspection to ensure that the goods entering the United States are in fact free of restricted and prohibited items.

Today, DNDO and CPB are fiscally constrained and are asking port operators to pay for Radiation Portal Monitors. As imports increase and container terminals reconfigure and expand, we need to ensure that we can continue to scan all of the cargo that is entering the United States. We would like to work with Congress and DHS to develop a plan to upgrade the obsolete equipment in our ports. Ports should not be responsible for paying for DHS owned, operated, and maintained equipment. If we are, we should be able to use grant funding to help offset those costs.

There has been a lot of discussion this morning about TWIC already, and we have worked closely with TSA and Coast Guard for many years on this important program. We strongly support TWIC and look forward to the day when it will be fully implemented.

The majority of TWICs will expire in the next 6 to 9 months. We are pleased that TSA has taken steps to address the issue of offering a reduced cost 3-year renewal option. However, our members are concerned that the lack of an updated threat assessment could compromise the security of our facilities.

We are also concerned that the renewal or extension process be convenient and efficient. TSA and their new contractor should again work closely with the maritime community on such issues as

enrollment center locations, bulk payment, and the availability of onsite enrollment and activation. When the reader rule is finally published, it is imperative that sufficient time be given to ports to implement the requirements and that adequate port security grant funding be available.

TWIC projects should be a top priority of the grant program once the reader rule is released. We encourage the Coast Guard to continue their proposed rulemaking process and for TSA to complete the reader testing and publish a qualified technology list.

Finally, as this committee considers future enhancements to the MTSA, we respectfully request you also consider a number of additional areas of concern that were outlined in my written statement.

Thank you for inviting us to testify on the 10th anniversary of the Maritime Transportation Security Act. We are indeed safer than we were 10 years ago, and the AAPA and its members remain committed to doing its part to protect America.

I would be happy to answer any questions you may have.

Mr. LOBIONDO. Thank you.

Mr. Koch.

Mr. KOCH. Thank you, Mr. Chairman and Congressman Larsen, for having this hearing. It is always appropriate to review where we are and where we are going.

My testimony, like other testimony here today, tries to set forth and discuss the multilayer risk assessment strategy that the DHS has developed cooperatively between CBP and the U.S. Coast Guard.

There is obviously a sophisticated system in place for vessel tracking using LRIT and other technology, obviously a regime in place to look at people and the security of the people, both on the ships that are coming in and out of U.S. ports as well as those working in the ports. There is a good strategy for vessel security plans, for port security plans, and, importantly, which we know has been an issue to this committee and Congress in general, for the cargo security as well, particularly containerized cargo. And I think DHS deserves credit for having constructed a system that is clearly the most sophisticated system of any trading nation in the world in terms of what data it acquires before vessel loading from the people who should have the best information available to them, so that Customs can undertake its cargo screening before vessel loading.

We continue to believe that before vessel loading screening is the proper strategy. Obviously, that requires getting the best data possible, and we think improvements have been made in that, and we think CBP is on the right track.

I guess what this basically says is that we believe that the strategy that has been put together makes sense. It is a sound strategy. The question really now should focus on the implementation of that strategy. Are we doing what we need to do to make that strategy actually effective?

Perhaps the most prominent question in that regard is the one that the subcommittee has already identified here today, and that is the TWIC, in terms of the personnel security. That obviously needs work, and I think everybody is looking forward to seeing

DHS deliver on the high priority it said it has on this and to having the proposed rule out before the end of this year.

One of the issues in terms of getting better information to the Government is how the Government uses that information. Obviously, you would probably be interested in having a sit-down with CBP to talk about how the National Targeting Center deals with all of the cargo information it gets. Our understanding is it has improved their screening capability quite a bit.

Obviously, the high-volume shippers of repetitive products are really not the kind of risk that is probably prominent in their minds. Whether it is Ford auto parts or Heineken beer coming in, those repetitive high-volume shippers are probably pretty low risk. It is the cargo from people you see less often, the shippers who don't have a good track record or who may appear in consolidated boxes coming through, that requires the kind of attention, requires the scanning of those boxes if CBP is not satisfied that it has enough information.

Our understanding is that the risk assessment system is working pretty well. Our understanding is that Customs is getting the information it wants. But that would be something you may want to be looking at as well.

One of the issues we have identified, which we also identified in the last hearing at which we were asked to testify, is getting CBP even better information about container cargo weights. We have a proposal at the IMO for that. We thank both you for having supported that proposal. It will be debated later this month at the IMO. The U.S. Government has agreed to cosponsor that proposal.

We think it makes good sense, certainly from a safety perspective, but we also believe that there is security value on this, and we understand that CBP has informed Coast Guard of their support for container weight verification for security risk screening purposes.

So all of those things being said, we believe the partnership between the industry and CBP and the Coast Guard is working quite well. There is good, open, honest dialogue. If there is a risk, it is communicated and people can act on it when they are reviewing vessel security plans or port security plans, and we continue to believe that the focus should be on the implementation of the strategy which we believe is a sound strategy.

Thank you, Mr. Chairman. I will be happy to take any questions.

Mr. LOBIONDO. Thank you, Mr. Koch.

Well, based on what you just said about working together and sharing ideas, do you feel the Government has reached out to the industry to understand how it works in the real world so that they can get a better perspective on what can be done for maritime security? You are pleased with that communications and reach-out?

Mr. KOCH. Yes, we are. I think when MTSA was just being rolled out there were bumps in the road which you might expect when a regime like that is coming together and being implemented. But the experience our members have had has been both the Coast Guard and CBP are quite professional; and when they have issues, the relationships are good.

Liner shipping might be a little bit different than other sectors because the vessels—the container ships and liner shipping vessels

are coming into ports every week—are regularly scheduled services. It is the same crews. It is the same captains. They are there time and time again. Schedule reliability is key, so the operators will bend over backwards to make sure the Government has got whatever it needs so they can stay on schedule; and if there is a question, the operators bend over backwards to try to make sure that the Coast Guard or CBP has what they need. We think that goes on in other sectors as well, but at least our experience has been the cooperation has been excellent.

Mr. LOBIONDO. On the TWICs, only U.S. mariners carry them. What in your view could be done to improve the security of the Merchant Marine credentials carried by foreign mariners?

Mr. KOCH. Well, it is a difficult diplomatic question. The U.S. Government has taken a position which is far more strict than many trading nations, which is that crewmen coming in on a foreign-flagged ship, if they are going to get off the ship in the U.S., have to have a visa. The ILO Maritime Labor Convention, which is about to enter into force internationally, takes a different view, which is that seafarers ought to be able to get off the ship without a visa. The U.S. Government, Australia, several other governments have said, no, the security of the United States requires that you go through the visa process and you have an interview and that that process be pursued.

So we believe the visa process satisfies the objectives of the Department of State and DHS in terms of ensuring that the crew on the ships coming to the U.S. have passed a sufficient security check that they are trustworthy.

I would point out that is different than many nations who have less security screening requirements on crewmen than the U.S. does.

Mr. LOBIONDO. Thank you.

Ms. Rooney, your port hosted a pilot program for the TWIC reader. Can you give us kind of a thumbnail sketch or a brief discussion on the pitfalls that the port encountered on that?

Ms. ROONEY. Yes, sir. There were a number of issues that we encountered with the pilot program, some of which were able to be worked out during the course of the pilot program and others that were still unresolved. But, in essence, they were technology issues. They were issues that allowed the reader to make a positive confirmation of the biometric that was stored in the card within a timely manner.

Many of the issues that were overcome had to do with user training and user knowledge and experience. So the first couple of times that a mariner or a truck driver or a longshoreman was presented with a TWIC reader, they fumbled over the process; and, over time, those were resolved. We are confident that those issues can be addressed and successfully overcome and we can move from this flash pass to the biometric credential that was originally intended.

Mr. LOBIONDO. Thank you.

Mr. Larsen.

Mr. LARSEN. Thank you, Mr. Chairman.

Ms. Rooney, with regards to both port security grant funding and the cost-share requirement, I have a couple questions.

First off, just some context. The Congress passed and the President signed recently a transportation bill where we went from 110 separate surface transportation accounts to approximately 30 or 40. We had to go some way to make that happen, but we thought, over time, even going back to the Democratic majority, to the Republican majority, that we needed to consolidate some of these accounts to give some more flexibility to recipients of the Federal dollars so they could choose more what they wanted to do, as opposed to saying this dollar can only do this and that dollar can only do that.

So that is the context of the question with regards to port security grant funding. I would just like to hear the point you want to make about why port security grant funding needs to stay separate, as opposed to being consolidated with other accounts other than it just should because it is.

Ms. ROONEY. I think the point that it needs to be separate is, by and large, because the maritime industry is largely owned and operated by the private sector. And the private sector is responsible for the security of the ports first and foremost in connection with their Federal, State, and local partners.

So when those private-sector entities—and, for example, in my port there are 185 facilities that are regulated by the Coast Guard. Approximately 170 of them are owned by private-sector operators. When those private-sector companies come forward in an environment where they are competing with the New York City Police Department, with the New York City Fire Department, with the Port Authority and others for dollars, they will be challenged to truly secure their facilities when other high-risk assets and activities are taking place in an area such as New York and New Jersey.

Mr. LARSEN. OK. All right.

And then with regards to the cost-share requirement, again, we have cost-share on surface transportation as well. Can you discuss a little bit more about the challenge of the cost-share in your situation?

Ms. ROONEY. Again, while many of the—while much of the responsibility at the facility level for security is with the private owners and operators, the public agencies provide layers of security over and above that. And when you look at the history of where the port security grant dollars have gone to in the last 4 or 5 years, much of that is going to public-sector agencies, all of whom are constrained with their own budgets today. So it becomes very difficult for public-sector agencies to provide the cost-share that is necessary. And, as a result, what we have seen historically for many years now is public-sector agencies pulling out of those grants and those risks no longer being mitigated because they cannot afford the cost-share.

Mr. LARSEN. OK. Thank you.

Sounds like everything is great in the World Shipping Council, Mr. Koch.

Mr. KOCH. If the companies could just learn how to be profitable, it would be even better.

Mr. LARSEN. With regards to MTSA, your attitude in the last hearing was the same as this one. It is like if it is a problem, we are going to fix it, we are going to work this thing out, we are going

to find a way to move cargo, because that is the job of the industry. And that is great. But can you talk a little bit about screening protocols under MTSA that shippers and carriers have to abide by to import cargoes in the U.S.?

This gets back to the 100 percent scanning of containers entering the U.S. Is the scanning—do you see that scanning as unnecessary, given cargo screening protocols, the 10+2 cargo screening protocols? Is 100 percent screening necessary? Should it be all risk-based? Where do you think we ought to be moving?

Mr. KOCH. Well, I think the 10+2 initiative did give CBP, obviously, a lot more information to do effective screening. And there is a semantic issue here. I think CBP would say they are screening 100 percent of all cargo before vessel loading.

Mr. LARSEN. Right.

Mr. KOCH. Screening meaning analyzing the information and making a judgment about risk.

It is the 100 percent scanning of a box, usually meant to be both radiation scanning and a kind of visual scan via x ray, gamma ray, or analogous technology. And frankly, the problem with such visual scanning of all containerized cargo is it is just not practical.

Whether it is needed or not I think is also a debate. Without meaning to be glib about it, I really don't think you need to scan every box of Heineken beer coming into the U.S., as an example, or Toyota auto parts coming into the U.S. I mean, I think the risk would not justify the expense of doing that.

The other problem, obviously, with the 100 percent proposal is it is an extraterritorial assertion of jurisdiction, and you are asking foreign governments to do something and incur the costs to do all of it. And there is resistance to that. They point out, with some degree of fairness, the U.S. doesn't undertake any such scanning for any of its exports, so why is it fair to require them to do that for their exports? And so there is a reciprocity issue there.

And then there is also the technology issue. The technology has not yet developed to a point where you could process that many containers through the system and continue to have the efficient flow of commerce.

The risk-based strategy is a strategy that from a practical perspective is your only choice. And so the question really I think is not to question the risk-based strategy so much as is to ensure that the agency, CBP, in charge of this, is getting the data that really makes sense. Is there data that they should be getting that they are not getting? And are they enforcing the existing obligations on people to give them the data?

In other words, you have an obligation for ocean carriers to file their manifests, their stowage plans, and all their container status messages. You have obligations on NVOs to file all of their manifests before vessel loading. And you have obligations on importers to file the 10 data elements identified in the 10+2 reg. Are they doing that?

Our understanding is they are. But I mean it would be worth checking into to make sure that they are getting the data that the strategy calls for.

Mr. LARSEN. Thank you, Mr. Chairman.

Mr. LOBIONDO. Ms. Rooney, Mr. Koch, I would like to thank you for being here this morning; and the subcommittee is adjourned. [Whereupon, at 10:31 a.m., the subcommittee was adjourned.]



**Statement of the Honorable Rick Larsen
Ranking Democratic Member**

**Coast Guard and Maritime Transportation Subcommittee Hearing on "Tenth Anniversary
of the Maritime Transportation Security Act: Are We Safer?"**

September 11, 2012

Mr. Chairman, thank you for convening this morning's hearing to assess the effectiveness of the Maritime Transportation Security Act, or MTSA, after ten years of implementation.

It is entirely appropriate that we evaluate MTSA today as we observe the 11th anniversary of the terrorist attacks of 9/11. There can be no more sober reminder that our work to protect our shores from terrorist threats requires our constant attention, creativity and dedication.

I also want to acknowledge the heroic contributions made by the United States Coast Guard on that horrific day eleven years ago to secure New York Harbor, and to oversee the successful evacuation of over 300,000 people from lower Manhattan after the collapse of the World Trade Center. Thank you, Admiral Servidio, to you and the entire Coast Guard family. On that day, the true definition of the Coast Guard motto, *Semper Paratus*, was made evident to all.

Mr. Chairman, border and transportation security is a pivotal function of the Federal Government in protecting the American people from terrorists and their instruments of destruction.

The maritime domain is particularly daunting in scale, totaling over 95,000 miles of shoreline, 300,000 square miles of waterways, and 10,000 miles of navigable waterways. There are over 360 ports, approximately 3,100 critical facilities, and more than 14,000 vessels in the domestic fleet alone. Each one of these presents a potential target for terrorist activity, so the complexity of securing these assets is a huge responsibility.

Aside from infrastructure, over 60 million Americans are employed within 100 miles of our coasts and contribute over \$4 billion annually to the nation's economy.

The response of Congress to the 9 11 attacks was followed by specific, targeted measures to protect the nation, such as the creation of the Transportation Security Administration. It also included the passage of MTSA which addressed the maritime domain.

MTSA did invoke new policies and strategies, including new requirements for passenger, crew and cargo screening, including the successful Customs' Trade Partnership Against Terrorism Program, or C-TPAT, and the Mega Ports Initiative, that has systematically enhanced detection capabilities for special nuclear and other radioactive materials in containerized cargo.

Additionally, greater use of technology to identify and track vessel movements; implementation of comprehensive biometric security measures; and the initiation of vulnerability assessments and creation of site-specific security plans, were all new innovations.

The question asked today, “Are We Safer?”, is as valid now as it was in the days and weeks immediately following 9/11. This basic question raises some other fundamental questions for which I will be interested to hear responses from our witnesses today.

Specifically, how do we know that we are, in fact, safer? By what metrics, are we making such determinations? And what are the economic side effects on foreign and domestic maritime commerce, and costs to the U.S. taxpayer? I will also be interested in learning whether our witnesses believe that adequate resources are being provided to support this vital responsibility.

As I mentioned during our hearing on Maritime Domain Awareness in July, unlike after 9/11 when resources were freely available to address deficiencies in homeland security, we operate now in an entirely different budget environment. Present fiscal constraints leave us little choice but to examine carefully the assets and resources we devote to maritime security, especially to the Coast Guard whose budget is already stretched thin over several different competing missions.

I have said this before and I will keep saying it: we cannot expect the Coast Guard to “do more with less.” The sad reality is the Coast Guard will be “doing less with less.” That is why we must spend effectively and wisely on those activities which provide the greatest risk reduction at lowest cost.

Obviously, challenges remain – TWIC readers and cargo scanning requirements immediately come to mind. Yet, as our present maritime security strategies continue to evolve, we should not allow frustration over some aspects to deter our efforts. We must press on to develop a maritime transportation security strategy that is comprehensive in scope, flexible in implementation, and adaptable to the changing tactics of those extremists who would seek to do us harm.

For if there is one indelible truth we have learned over the past ten years, it is that the terrorists will not tire in their efforts to probe, adapt, and exploit our vulnerabilities. Like the Coast Guard, we must remain *Semper Paratus*. Thank you.

###

U. S. Department of
Homeland Security
United States
Coast Guard



Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-0921
Phone: (202) 372-3500
FAX: (202) 372-2311

**DEPARTMENT OF HOMELAND SECURITY
U. S. COAST GUARD
STATEMENT OF**

REAR ADMIRAL JOSEPH A. SERVIDIO

**ON
MARITIME TRANSPORTATION SECURITY ACT: TEN YEARS LATER
BEFORE THE
COAST GUARD AND MARITIME TRANSPORTATION SUBCOMMITTEE
U. S. HOUSE OF REPRESENTATIVES**

SEPTEMBER 11, 2012

Introduction

Good morning Mr. Chairman and distinguished Members of the Subcommittee. It is a pleasure to be here today to discuss the Coast Guard's role in securing our maritime infrastructure since the events of 9/11 and the subsequent passage of the *Maritime Transportation Security Act (MTSA) of 2002*.

The United States is a maritime nation. We have one of the world's longest coastlines, measuring more than 95,000 miles, and the world's largest Exclusive Economic Zone (EEZ). The U.S. marine transportation system (MTS) is comprised of 361 ports and thousands of miles of maritime thoroughfares that support 95 percent of U.S. foreign trade. According to the Coast Guard's Notice of Arrival database, most of that trade is transported on over 7,500 vessels that make more than 60,000 visits to U.S. ports annually, and 2011 statistics exceeded these averages significantly. In 2011, a reported total of 9,326 individual vessels, from 85 different Flag Administrations, made 79,031 port calls to the United States.

Recognizing the importance of the U.S. MTS, the Coast Guard has made progress in securing America's waterways and supporting an open and resilient commercial environment. The men and women of the Coast Guard and the other components of the Department of Homeland Security (DHS) remain committed to improving maritime security through continued interagency cooperation and collaboration with federal, state, local, international and industry partners.

Reducing Maritime Risk

The Coast Guard's security goal is to prevent the exploitation of, or terrorist attacks within, the U.S. maritime domain. Doing so requires a risk-based approach to identify and intercept external threats before they reach U.S. shores, and to detect and respond to internal threats before they cause a maritime transportation security incident (TSI).

The Coast Guard accomplishes this by participating in layered, multi-agency security operations nationwide, including regulatory development and partnership activities with the private sector mandated by MTSA. These activities have strengthened the security posture and reduced the vulnerability of our ports.

The Coast Guard defines maritime security risk as a function of threat, vulnerability, and consequence. Due to its size, complexity, and impact on the Nation's economy, the U.S. MTS is a highly valuable and vulnerable target for attack by terrorists or exploitation by transnational criminal organizations.

- **Threat:** Although terrorists have never conducted a successful attack in a U.S. port or within the maritime borders of the United States, and current reporting does not indicate a near-term maritime terrorism threat to the U.S. homeland, this does not preclude the possibility of future attacks.
- **Vulnerability:** The vastness of this system and its widespread and diverse critical infrastructure leave the nation vulnerable to terrorist acts within our ports, waterways, and coastal zones, as well as exploitation of maritime commerce as a means of transporting terrorists and their weapons.
- **Consequence:** The closure of one or more high volume ports for a significant period of time would create a costly disruption to commerce. A direct attack on certain critical infrastructure in high density ports could produce mass casualties and long-term environmental damage.

MTSA – Ten Years Later...Recapping the Coast Guard's Accomplishments

Scope of the Regulated Industry

As of August 17, 2012, there are 3,161 facilities regulated by MTSA and 14,553 MTSA-regulated domestic vessels in service. Under the MTSA regulations¹, facilities and vessels have designated individuals with security responsibilities, including company security officers, facility security officers, and vessel security officers². These individuals must be familiar with, and are responsible for, implementation of the specific security measures outlined in their facility/vessel security plans and they must be knowledgeable in emergency preparedness, the conduct of security audits, and security exercises. In addition, facility and vessel security officers must have training in: security assessment methodologies; current security threats and patterns; recognizing and detecting dangerous substances and devices, recognizing characteristics and behavioral patterns of persons who are likely to threaten security; and techniques used to circumvent security measures.

In accordance with the *Security and Accountability For Every Port Act of 2006*, the Coast Guard conducts verifications on facilities within each 12 month period, including a minimum of:

1. One announced annual MTSA compliance examination for each facility;
2. One unannounced facility security spot check for each facility; and
3. Where the facility security spot check or deficiency or violation history warrants, an unannounced MTSA annual compliance examination.

Additionally, Captains of the Port may require additional compliance exams or security spot checks beyond these mandated requirements at their discretion based upon resource availability, local risk, and mission priorities.

¹ MTSA regulations begin at 33 CFR 101, Subchapter H; 68 FR 39287 / July 1, 2003

² 33 CFR Subchapter H, parts 104, 105 and 106

To verify compliance with the Transportation Worker Identification Credential (TWIC) requirements aboard U.S. flag vessels regulated under MTSA, the Coast Guard conducts TWIC verifications as part of annual U.S. flag vessel inspections.

Performance Highlights

In FY 2011 the Coast Guard:

- Conducted over 10,400 annual inspections of U.S. flagged vessels inspected and certificated in accordance with 46 Code of Federal Regulation (CFR) § 2.01 which provides the Coast Guard authorities over many aspects of domestic vessel safety, manning, and rules of operation.
- Performed over 6,500 inspections at facilities to ensure compliance, identifying over 2,250 deficiencies of safety, security, and environmental protection regulations.
- Conducted 10,129 Safety of Life at Sea (SOLAS) safety exams and 8,909 International Ship and Port Facility Security (ISPS) Code exams, which is an amendment to the SOLAS treaty.
- Completed over 26,500 container inspections, identifying more than 2,220 deficiencies that led to 915 cargo or container shipments being placed on hold until dangerous conditions were corrected.
- Verified approximately 70,000 TWICs.

Regulations Update

The Coast Guard is proud of its regulatory achievements to date, having issued 13 Final Rules (FR) related to the MTSA. The bulk of the MTSA provisions were implemented in the rules published in October 2003. We continue to engage in rulemaking to further bolster our security regimes. The impact and value of some of these regulations are highlighted throughout the remainder of my testimony.

RIN	Title	FR Citation	FR Date	Effective Start Date	Status
1625-AA30	Territorial Seas, Navigable Waters, and Jurisdiction	68 FR 42595	7/18/2003	8/18/2003	Final Rule
1625-AA42	Area Maritime Security	68 FR 60472	10/22/2003	11/21/2003	Final Rule
1625-AA43	Facility Security	68 FR 60515	10/22/2003	11/21/2003	Final Rule
1625-AA46	Vessel Security	68 FR 60483	10/22/2003	11/19/2003	Final Rule
1625-AA67	Automatic Identification System; Vessel Carriage Requirement	68 FR 60559	10/22/2003	11/21/2003	Final Rule
1625-AA68	Outer Continental Shelf Facility Security	68 FR 60545	10/22/2003	11/21/2003	Final Rule
1625-AA69	Implementation of National Maritime Security Initiatives	68 FR 60448	10/22/2003	11/21/2003	Final Rule
1625-AA86	Unauthorized Entry Into Cuban Territorial Waters	69 FR 41367	7/8/2004	7/2/2004	Final Rule

1625-AA82	Notification of Arrival in U.S. Ports; Certain Dangerous Cargoes; Electronic Submission	69 FR 51176	8/18/2004	9/17/2004	Temporary Rule
1625-AA96	Notification of Arrival in U.S. Ports; Certain Dangerous Cargoes; Electronic Submission	70 FR 74663	12/16/2005	1/17/2006	Interim Rule
1625-AA20	Deepwater Ports	71 FR 57644	9/29/2006	9/29/2006	Final Rule
1625-AB00	Long Range Identification and Tracking of Ships	73 FR 23310	4/29/2001	5/29/2008	Final Rule
1625-AB02	Consolidation of Merchant Mariner Qualification Credentials	74 FR 11196	3/16/2009	4/15/2009	Final Rule
1625-AB19	Crewmember Identification Documents	74 FR 19135	4/28/2009	5/28/2009	Final Rule
1625-AA93	Notification of Arrival in U.S. Ports; Certain Dangerous Cargoes	75 FR 59617	9/28/2010	10/28/2010	Final Rule

Maintaining and Overseeing the Maritime Security Regime

To help prevent terrorist attacks, we have developed and continue to improve an effective maritime security regime – both domestically and internationally. This element of our strategy includes initiatives related to MTSA regulatory enforcement, International Maritime Organization regulations, such as the ISPS Code, as well as global supply chain security and identity security processes.

Before 9/11, we had no formal international or domestic maritime security regime for ports, port facilities, or ships – with the exception of cruise ships. Partnering with domestic and international stakeholders, we now have comprehensive domestic and international security regimes in place³.

³ 33 CFR 101.100(a)(2) states one of the purposes of the subchapter is to align, where appropriate, the requirements of domestic maritime security regulations with the international maritime security standards in the International Convention for the Safety of Life at Sea, 1974 (SOLAS Chapter XI-2) and the International Code for the Security of Ships and Port Facilities, parts A and B, adopted on 12 December 2002.³ 68 FR 39278, July 1, 2003, as amended at 68 FR 60470, October 22, 2003 [*see generally* 33 CFR Subchapter H-Maritime Security, 68 FR 39240, July 1, 2003].

These have been in force since July 1, 2004. In executing the requirements of the MTSA and the ISPS Code, the Coast Guard:

- Reviewed and approved over 11,000 domestic vessel security plans and 3,100 domestic facility security plans;
- Oversaw the development of 43 Area Maritime Security Plans and Committees;
- Completed domestic port security assessments for all U.S. ports using the Maritime Security Risk Analysis Model;
- Visited almost 160 foreign countries to assess the effectiveness of port security measures and implementation of ISPS Code requirements; and
- Oversaw the continuing development of the National Maritime Security Plan, which is one of eight supporting implementation plans of the National Strategy for Maritime Security established through HSPD-41/HSPD-13 and its Maritime Security Policy Coordinating Committee.

MTSA and the ISPS Code remain landmark achievements within the maritime industry. Through a variety of measures of regulatory requirements, these two regimes complement each other and have gone far to reduce vulnerabilities within the global marine transportation system, the general framework of which includes:

- *Physical Security.* The first pillar of this framework is physical security. Through the implementation of the MTSA regulations, we have significantly hardened the physical security of our ports. Roughly 3,100 of the nation's highest risk port facilities have implemented mandatory access control measures to control who has access to restricted areas of these facilities. Owners and operators are now required, under Federal regulations⁴ to implement screening protocols for ensuring cargo-transport vehicles and persons entering the facilities are inspected to deter the unauthorized introduction of dangerous substances and devices. At the facility gates, containers are required to be checked for evidence of tampering and cargo seals are checked. Similar measures are in effect for commercial vessels, such as: cruise ships; ferries; oil and chemical tankers; and cargo vessels⁵.
- *Identity Security.* We must know and trust those who are provided unescorted access to our port facilities and vessels. The 9/11 Commission report noted that the September 11th hijackers obtained and used government-issued identification cards such as driver's licenses. The Commission recommended that forms of identification be made more secure. Congress addressed this issue in MTSA by mandating the development of the biometrically enabled TWIC. The Coast Guard has worked very closely with the Transportation Security Administration (TSA), the lead agency for implementation of the TWIC Program. For the first time in the maritime environment, TWIC established uniform vetting of maritime workers based on recognized standards. Port security officers across the country now encounter a single, recognizable, tamper-resistant credential, rather than hundreds of different identity cards, allowing them to make more informed access control decisions. Furthermore, the Coast Guard has updated the merchant mariner credentialing regulations and related policies to better align them with the capabilities of the TWIC.

⁴ (33 CFR 105; 68 FR 39322 / July 1, 2003)

⁵ (33 CFR 104; 68 FR 39302 / July 1, 2003)

The Coast Guard is also working on a rulemaking project to address the requirements of Section 809 of the *Coast Guard Authorization Act of 2010* – which excludes certain mariners from the statutory requirement to obtain and hold a TWIC in order to receive a merchant mariner credential. The Coast Guard remains fully supportive of this program and is developing a rulemaking project that would leverage the biometric aspects of the credential by the use of card readers at certain MTSA-regulated facilities and vessels.

- *Global Supply Chain Security*: Cargo security involves ensuring all cargo bound for the U.S. is legitimate and was properly supervised from the point of origin, through its sea transit and delivery to the final destination in the U.S. DHS has initiated a robust global supply chain security effort with our domestic and international partners in recognition of the ripple effects that are felt worldwide if a disruption in commerce occurs. This effort is directed toward a global system that is secure, efficient, and resilient as outlined in the U.S. *National Strategy for Global Supply Chain Security*.

Collaborative Efforts

The Coast Guard has worked in concert with U.S. Customs and Border Protection (CBP) to enhance maritime security through a risk-based approach. As part of this effort, the Coast Guard oversees the training and identity verification of people who are moving the cargo. To facilitate this process, the trade community can file required passenger and crew information via an electronic notice of arrival and departure system⁶. In addition, when cargo is moved on the waterborne leg of the trade route, the Coast Guard has oversight of the cargo's care and carriage on the vessels and within the U.S. port facility. Using the information provided through the Coast Guard's 96-hour notice of arrival requirement⁷ and CBP's mandatory advance electronic cargo manifest rule⁸, the Coast Guard works with CBP to identify and evaluate cargo risks well in advance, and when necessary, control vessels and cargo that may pose a threat. The Coast Guard also works in concert with CBP at the National Targeting Center to take appropriate action when notified of a cargo of interest.

The Coast Guard has aligned our regulatory and policy development efforts with CBP and TSA. In addition, we continue to meet regularly to discuss policy and we participate on inter-agency regulatory development teams. Between DHS, CBP, and the Coast Guard, we coordinate the work of our various Federal Advisory Committees so that we all appreciate and address the trade community's concerns and priorities. We continue to monitor compliance and carefully note issues and lessons learned for future improvements to the regulatory framework now that MTSA and the ISPS have been fully implemented.

Improved Response and Recovery Posture

Finally, MTSA and related security efforts have improved our ability to respond to and aid in recovery and response to all terrorist attacks and natural disasters. Response and recovery protocols, established and exercised with our Federal, state, local and industry partners, build a resilient maritime community, which is able to recover more quickly from natural disasters, accidents, or attacks. In fact, the Coast Guard is actively promoting port resilience and trade recovery, within our domestic ports, with Canada, and with the larger international community via the International Maritime Organization, the Asia-Pacific Economic Cooperation forum, and in partnership with CBP, and the World Customs Organization.

⁶ 19 CFR part 4.7b

⁷ 33 CFR part 160.212

⁸ 19 CFR part 4.7a(c)(4)(xv) and (xvi)

For example, the Coast Guard's efforts with Canada include: supply chain security, resiliency, and marine safety in developing joint strategies to facilitate the sharing of information and resources during emergencies; the dissemination of best practices; and the development of clear lines of communication consistent with agreed information elements.

At the local level, each port is ready with port-specific and even sub-area specific, response plans. All law enforcement agencies, public service providers, and port stakeholders have participated in the plan development process. Partnering with various port and industry organizations through Area Maritime Security Committees, Harbor Safety Committees and Port Readiness Committees provide continuing opportunities for cooperation and collaboration for improving the security, safety, and resiliency of our ports.

Conclusion

Since 9/11, we have worked to strengthen the security of the maritime transportation system and global supply chains. The tremendous success in this endeavor is due, in large part, to cooperation among Federal, state, and local government and industry partners. We look forward to working with Congress to continue to enhance maritime security.

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

United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Coast Guard
and Maritime Transportation, Committee
on Transportation and Infrastructure,
House of Representatives

For Release on Delivery
Expected at 9:30 a.m. EST
Tuesday, September 11, 2012

MARITIME SECURITY

Progress and Challenges Ten Years after the Maritime Transportation Security Act

Statement of Stephen L. Caldwell, Director
Homeland Security and Justice



September 11, 2012



Highlights of GAO-12-1009T, a testimony for the Subcommittee on Coast Guard and Maritime Transportation, Committee on Transportation and Infrastructure, House of Representatives

MARITIME SECURITY

Progress and Challenges 10 Years After the Maritime Transportation Security Act

Why GAO Did This Study

Ports, waterways, and vessels handle billions of dollars in cargo annually and an attack on this maritime transportation system could impact the global economy. November 2012 marks the 10-year anniversary of MTSA, which required a wide range of security improvements. DHS is the lead federal department responsible for implementing MTSA and it relies on its component agencies, such as the Coast Guard and CBP, to help implement the act. The Coast Guard is responsible for U.S. maritime security interests and CBP is responsible for screening arriving vessel crew and cargo. This testimony summarizes GAO's work on implementation of MTSA requirements over the last decade and addresses (1) progress the federal government has made in improving maritime security and (2) key challenges that DHS and its component agencies have encountered in implementing maritime security-related programs. GAO was unable to identify all related federal spending, but estimated funding for certain programs. For example, from 2004 through May 2012, CBP received over \$390 million to fund its program to partner with companies to review the security of their supply chains. This statement is based on GAO products issued from July 2002 through August 2012, as well as updates on the status of recommendations made and budget data obtained in August 2012.

What GAO Recommends

GAO has made recommendations to DHS in prior reports and testimonies to strengthen its maritime security programs. DHS generally concurred and has implemented or is in the process of implementing them.

View GAO-12-1009T. For more information, contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov

What GAO Found

GAO's work has shown that the Department of Homeland Security (DHS), through its component agencies, particularly the Coast Guard and U.S. Customs and Border Protection (CBP), have made substantial progress in implementing various programs that, collectively, have improved maritime security. In general, GAO's work on maritime security programs falls under four areas: (1) security planning, (2) port facility and vessel security, (3) maritime domain awareness and information sharing, and (4) international supply chain security. DHS has, among other things, developed various maritime security programs and strategies and has implemented and exercised security plans. For example, the Coast Guard has developed Area Maritime Security Plans around the country to identify and coordinate Coast Guard procedures related to prevention, protection, and security response at domestic ports. In addition, to enhance the security of U.S. ports, the Coast Guard has implemented programs to conduct annual inspections of port facilities. To enhance the security of vessels, both CBP and the Coast Guard receive and screen advance information on commercial vessels and their crews before they arrive at U.S. ports and prepare risk assessments based on this information. Further, DHS and its component agencies have increased maritime domain awareness and have taken steps to better share information by improving risk management and implementing a vessel tracking system, among other things. For example, in July 2011, CBP developed the Small Vessel Reporting System to better track small boats arriving from foreign locations and deployed this system to eight field locations. DHS and its component agencies have also taken actions to improve international supply chain security, including developing new technologies to detect contraband, implementing programs to inspect U.S.-bound cargo at foreign ports, and establishing partnerships with the trade industry community and foreign governments.

Although DHS and its components have made substantial progress, they have encountered challenges in implementing initiatives and programs to enhance maritime security since the enactment of the Maritime Security Transportation Act (MTSA) in 2002 in the areas of: (1) program management and implementation; (2) partnerships and collaboration; (3) resources, funding, and sustainability; and (4) performance measures. For example, CBP designed and implemented an initiative that placed CBP staff at foreign seaports to work with host nation customs officials to identify high-risk, U.S.-bound container cargo, but CBP initially did not have a strategic or workforce plan to guide its efforts. Further, the Coast Guard faced collaboration challenges when developing and implementing its information management system for enhancing information sharing with key federal, state, and local law enforcement agencies because it did not systematically solicit input from these stakeholders. Budget and funding decisions have also affected the implementation of maritime security programs. For example, Coast Guard data indicate that some of its units are not able to meet self-imposed standards related to certain security activities—including boarding and escorting vessels. In addition, DHS has experienced challenges in developing effective performance measures for assessing the progress of its maritime security programs. For example, the Coast Guard developed a performance measure to assess its performance in reducing maritime risk, but has faced challenges using this measure to inform decisions.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the Department of Homeland Security's (DHS) and other agencies' implementation of the Maritime Transportation Security Act of 2002 (MTSA).¹ Ports, waterways, and vessels handle billions of dollars in cargo annually, and an attack on our nation's maritime transportation system could have dire consequences. Ports are inherently vulnerable to terrorist attacks because of their size, general proximity to metropolitan areas, the volume of cargo being processed, and the ready access the ports have to transportation links into the United States. An attack on a port could have a widespread impact on international trade and the global economy. Balancing security concerns with the need to facilitate the free flow of people and commerce remains an ongoing challenge for the public and private sectors alike.

November 2012 will mark the 10th anniversary of the enactment of MTSA, which requires a wide range of security improvements designed to help protect the nation's ports, waterways, and coastal areas from terrorist attacks by requiring a wide range of security improvements. Prior to the terrorist attacks of September 11, 2001, federal attention at ports tended to focus on navigation and safety issues, such as dredging channels and environmental protection.

DHS is the lead federal agency responsible for implementing MTSA requirements and it relies on a number of its component agencies that have responsibilities related to maritime security, as follows.²

- **U.S. Coast Guard:** The Coast Guard has primary responsibility for ensuring the safety and security of U.S. maritime interests and leading homeland security efforts in the maritime domain. In this capacity, among other things, the Coast Guard conducts port facility and commercial vessel inspections, leads the coordination of maritime

¹Pub. L. No. 107-295, 116 Stat. 2064.

²Immigration and Customs Enforcement (ICE) also contributes to maritime security in that its mission is to detect and prevent terrorist and criminal acts by targeting the people, money, and materials that support terrorist and criminal networks. In this capacity, ICE contributes to DHS border security efforts, including in the maritime environment, even though its main focus is not on interdicting or screening operations.

information sharing efforts, and promotes domain awareness in the maritime environment.³

- **U.S. Customs and Border Protection (CBP):** CBP is responsible for the screening of incoming vessels' crew and maritime cargo for the presence of contraband, such as weapons of mass destruction, illicit drugs, or explosives, while facilitating the flow of legitimate trade and passengers.
- **Transportation Security Administration (TSA):** TSA has responsibility for managing the Transportation Worker Identification Credential program, which is designed to control the access of maritime workers to regulated maritime facilities in the United States.⁴
- **Domestic Nuclear Detection Office (DNDO):** DNDO is responsible for acquiring and supporting the deployment of radiation detection equipment, including radiation portal monitors at domestic seaports to support the scanning of cargo containers before they enter U.S. commerce.
- **Federal Emergency Management Agency (FEMA):** FEMA is responsible for administering grants to improve the security of the nation's highest risk port areas.

It is important to note that some of these agencies were made responsible for implementing MTSA requirements in the midst of the most extensive federal reorganization in over 50 years, as most were reorganized into DHS in March 2003, when DHS began operating—less than 5 months after MTSA enactment. This reorganization introduced new chains of command and reporting responsibilities. MTSA implementation also involved coordination with other executive branch agencies, including the Departments of Justice, State, and Transportation.

³Maritime domain awareness is the understanding by stakeholders involved in maritime security of anything associated with the global maritime environment that could adversely affect the security, safety, economy or environment of the United States.

⁴ The Coast Guard is responsible for enforcement of the Transportation Worker Identification Credential program.

In 2006, the Security and Accountability For Every Port Act of 2006 (SAFE Port Act) became law.⁵ The act amended MTSA and required DHS to develop, implement, and update, as appropriate, a strategic plan to enhance the security of the international supply chain—the flow of goods from manufacturers to retailers.⁶ Further, the SAFE Port Act required DHS to establish pilot projects at three ports to test the feasibility of scanning 100 percent of U.S.-bound cargo containers at foreign ports.⁷

My statement today summarizes our work on maritime security since the enactment of MTSA and is focused on

- progress the federal government has made in improving maritime security, and
- key challenges that DHS and its component agencies have encountered in implementing maritime security-related programs.

We were unable to identify all federal spending for these purposes, but were able to estimate obligations or expenditures for certain programs. For example, we were not able to determine obligations for many of the MTSA-related Coast Guard programs—such as port security exercises—because they are funded at the account level (i.e., operating expenses) rather than as specific line items. However, we were able to estimate obligations or expenditures in some instances. For example, from fiscal years 2004 through May 2012, CBP obligated over \$390 million for a voluntary program that enables CBP officials to work in partnership with private companies to review and validate companies' practices for securing their international supply chains.

⁵ Pub. L. No. 109-347, 120 Stat. 1884.

⁶ The SAFE Port Act required DHS to report to Congress on this strategic plan by July 2007, with an update of the strategic plan to be submitted to Congress 3 years later. See 6 U.S.C. § 941(a), (g).

⁷ 6 U.S.C. § 981. Related to this SAFE Port Act requirement, in August 2007, the Implementing Recommendations of the 9/11 Commission Act of 2007 was enacted, which required, among other things, that by July 2012, 100 percent of all U.S.-bound cargo containers be scanned at foreign ports, with possible extensions for ports at which certain conditions exist. See Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (amending 6 U.S.C. § 982(b)). Such extensions have been granted, as explained later in this statement.

In addition to the statement, appendix I summarizes select programs and activities that have been implemented since November 2002 to address maritime security and the associated expenditures, where information was available. The appendix also includes key findings from our work regarding these programs and activities in the last 10 years, as well as the progress that DHS and its component agencies have made in responding to our recommendations.

This statement is based primarily on reports and testimonies we have issued from August 2002 through July 2012 related to maritime, port, vessel, and cargo security efforts of the federal government, and other related aspects of implementing MTSA requirements. The statement also includes selected updates—conducted in August 2012—to the information provided in these previously-issued products on the actions DHS and its component agencies have taken to address recommendations made in these products. Where available, we have also included information on the funding for key maritime security related programs through May 2012. This additional information can be seen in appendix I. We conducted the work in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To perform the work, we visited domestic and overseas ports; reviewed agency program documents, port security plans, and postexercise reports, and other documents; and interviewed officials from the federal, state, local, private, and international sectors, among other things. The officials were from a wide variety of stakeholders to include the Coast Guard, CBP, TSA, port authorities, terminal operators, vessel operators, foreign governments, and international trade organizations. Further details on the scope and methodology for the previously issued reports and testimonies are available within each of the published products.

DHS Has Made Substantial Progress in Improving Maritime Security

Our work has shown that DHS and its component agencies—particularly the Coast Guard and CBP—have made substantial progress in implementing various programs that, collectively, have improved maritime security. In general, our maritime security-related work has addressed four areas: (1) national and port-level security planning, (2) port facility and vessel security, (3) maritime domain awareness and information

sharing, and (4) international supply chain security. Detailed examples of progress in each of these four areas are discussed below.

National and Port-Level Security Planning

The federal government has made progress in national and port-level security planning by, for example, developing various maritime security strategies and plans, and conducting exercises to test these plans.

- **Developing national-level security strategies:** The federal government has made progress developing national maritime security plans. For example, the President and the Secretaries of Homeland Security, Defense, and State approved the National Strategy for Maritime Security and its supporting plans in 2005. The strategy has eight supporting plans that are intended to address the specific threats and challenges of the maritime environment, such as maritime commerce security. We reported in June 2008 that these plans were generally well developed and, collectively, included desirable characteristics, such as (1) purpose, scope, and methodology; (2) problem definition and risk assessment; (3) organizational roles, responsibilities, and coordination; and (4) integration and implementation. Including these characteristics in the strategy and its supporting plans can help the federal government enhance maritime security.⁸ For example, better problem definition and risk assessment provide greater latitude to responsible parties for developing approaches that are tailored to the needs of their specific regions or sectors. In addition, in April 2008 DHS released its *Small Vessel Security Strategy*, which identified the gravest risk scenarios involving the use of small vessels for launching terrorist attacks, as well as specific goals where efforts can achieve the greatest risk reduction across the maritime domain.⁹
- **Developing port-level security plans:** The Coast Guard has developed Area Maritime Security Plans (AMSP) around the country to enhance the security of domestic ports. AMSPs, which are developed by the Coast Guard with input from applicable governmental and private entities, serve as the primary means to

⁸GAO, *Maritime Security: National Strategy and Supporting Plans Were Generally Well-Developed and Are Being Implemented*, GAO-08-672 (Washington, D.C.: June 20, 2008).

⁹Department of Homeland Security, *Small Vessel Security Strategy* (Washington, D.C., April 2008).

identify and coordinate Coast Guard procedures related to prevention, protection, and security response. Implementing regulations for MTSA specified that these plans include, among other things, (1) operational and physical security measures that can be intensified if security threats warrant it; (2) procedures for responding to security threats, including provisions for maintaining operations at domestic ports; and (3) procedures to facilitate the recovery of the maritime transportation system after a security incident.¹⁰ We reported in October 2007 that to assist domestic ports in implementing the AMSPs, the Coast Guard provided a common template that specified the responsibilities of port stakeholders.¹¹ Further, the Coast Guard has established Area Maritime Security Committees—forums that involve federal and nonfederal officials who identify and address risks in a port—to, among other things, provide advice to the Coast Guard for developing the associated AMSPs. These plans provide a framework for communication and coordination among port stakeholders and law enforcement officials and identify and reduce vulnerabilities to security threats throughout the port area.

- **Exercising security plans:** DHS has taken a number of steps to exercise its security plans. The Coast Guard and the Area Maritime Security Committee are required to conduct or participate in exercises to test the effectiveness of AMSPs at least once each calendar year, with no more than 18 months between exercises.¹² These exercises are designed to continually improve preparedness by validating information and procedures in the AMSPs, identifying strengths and weaknesses, and practicing command and control within an incident command/unified command framework. To aid in this effort, the Coast Guard initiated the Area Maritime Security Training and Exercise Program in October 2005. This program is designed to involve all port stakeholders in the implementation of the AMSPs. Our prior work has shown that the Coast Guard has exercised these plans and that, since development of the AMSPs, all Area Maritime Security Committees have participated in a port security exercise.¹³ Lessons learned from

¹⁰ 33 C.F.R. § 103.505.

¹¹ GAO, *Maritime Security: The SAFE Port Act and Efforts to Secure Our Nation's Seaports*, GAO-08-86T (Washington, D.C.: Oct. 4, 2007).

¹² 33 C.F.R. § 103.515.

¹³ GAO, *Maritime Security: The SAFE Port Act: Status and Implementation One Year Later*, GAO-08-126T (Washington, D.C.: Oct. 30, 2006).

the exercises are incorporated into plans, which Coast Guard officials said lead to planning process improvements and better plans.

Port Facility and Vessel Security

In addition to developing security plans, DHS has taken a number of actions to identify and address the risks to port facilities and vessels by conducting facility inspections and screening and boarding vessels, among other things.

- **Requiring facility security plans and conducting inspections:** To enhance the security of port facilities, the Coast Guard has implemented programs to require port facility security plans and to conduct annual inspections of the facilities. Owners and operators of certain maritime facilities are required to conduct assessments of security vulnerabilities, develop security plans to mitigate these vulnerabilities, and implement measures called for in their security plans. Coast Guard guidance calls for at least one announced and one unannounced inspection each year to ensure that security plans are being followed. We reported in February 2008, on the basis of these inspections, the Coast Guard had identified and corrected port facility deficiencies. For example, the Coast Guard identified deficiencies in about one-third of the port facilities inspected from 2004 through 2006, with deficiencies concentrated in certain categories, such as failing to follow facility security plans for port access control.¹⁴ In addition to inspecting port facilities, the Coast Guard also conducts inspections at offshore facilities, such as oil rigs. Requiring the development of these security plans and inspecting facilities to correct deficiencies helps the Coast Guard mitigate vulnerabilities that could be exploited by those with the intent to kill people, cause environmental damage, or disrupt transportation systems and the economy.
- **Issuing facility access cards:** DHS and its component agencies have made less progress in controlling access to secure areas of port facilities and vessels. To control access to these areas, DHS was required by MTSA to, among other things, issue a transportation worker identification credential that uses biometrics, such as

¹⁴GAO, *Maritime Security: Coast Guard Inspections Identify and Correct Facility Deficiencies, but More Analysis Needed of Program's Staffing, Practices, and Data*, GAO-08-12 (Washington, D.C.: Feb. 14, 2008).

fingerprints.¹⁵ TSA had already initiated a program to create an identification credential that could be used by workers in all modes of transportation when MTSAs were enacted. This program, called the Transportation Worker Identification Credential (TWIC) program, is designed to collect personal and biometric information to validate workers' identities and to conduct background checks on transportation workers to ensure they do not pose a threat to security. We reported in November 2009 that TSA, the Coast Guard, and the maritime industry took a number of steps to enroll 1,121,461 workers in the TWIC program, or over 93 percent of the estimated 1.2 million potential users, by the April 15, 2009, national compliance deadline.¹⁶ However, as discussed later in this statement, internal control weaknesses governing the enrollment, background check process, and use of these credentials potentially limit the program's ability to provide reasonable assurance that access to secure areas of MTSAs-regulated facilities is restricted to qualified individuals.

- **Administering the Port Security Grant Program:** DHS has taken steps to improve the security of port facilities by administering the Port Security Grant Program. To help defray some of the costs of implementing security at ports around the United States, this program was established in January 2002 when TSA was appropriated \$93.3 million to award grants to critical national seaports.¹⁷ MTSAs codified the program when it was enacted in November 2002.¹⁸ The Port Security Grant Program awards funds to states, localities, and private port operators to strengthen the nation's ports against risks associated with potential terrorist attacks. We reported in November 2011 that, for fiscal years 2010 and 2011, allocations of these funds were based on DHS's risk model and implementation decisions, and were made largely in accordance with risk. For example, we found

¹⁵46 U.S.C. § 70105.

¹⁶GAO, *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers*, GAO-10-43 (Washington, D.C.: Nov. 18, 2009).

¹⁷Pub. L. No. 107-117, 115 Stat. 2230, 2327 (2002).

¹⁸46 U.S.C. § 70107.

that allocations of funds to port areas were highly positively correlated to port risk, as calculated by DHS's risk model.¹⁹

- **Reviewing vessel plans and conducting inspections:** To enhance vessel security, the Coast Guard has taken steps to help vessel owners and operators develop security plans and the Coast Guard regularly inspects these vessels for compliance with the plans. MTSA requires certain vessel owners and operators to develop security plans, and the Coast Guard is to approve these plans.²⁰ Vessel security plans are to designate security officers; include information on procedures for establishing and maintaining physical security, passenger and cargo security, and personnel security; describe training and drills, and identify the availability of appropriate security measures necessary to deter transportation security incidents, among other things. The Coast Guard took several steps to help vessel owners and operators understand and comply with these requirements. In particular, the Coast Guard (1) issued updated guidance and established a "help desk" to provide stakeholders with a single point of contact, both through the Internet and over the telephone; (2) hired contractors to provide expertise in reviewing vessel security plans; and (3) conducts regular inspections of vessels. For example, we reported in December 2010 that, according to Coast Guard officials, the Coast Guard is to inspect ferries four times per year. The annual security inspection, which may be combined with a safety inspection and typically occurs when the ferry is out of service, and the quarterly inspections, which are shorter in duration, and generally take place while the ferry remains in service. During calendar years 2006 through 2009, the most recent years for which we have data, the Coast Guard reports that it conducted over 1,500 ferry inspections.²¹ These security plan reviews and inspections have enhanced vessel security.
- **Conducting vessel crew screenings:** To enhance the security of port facilities, both CBP and the Coast Guard receive and screen advance information on commercial vessels and their crew before

¹⁹GAO, *Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened*, GAO-12-47 (Washington, D.C.: Nov. 17, 2011).

²⁰46 U.S.C. § 70103(c)

²¹GAO, *Maritime Security: Ferry Security Measures Have Been Implemented, but Existing Studies Could Further Enhance Security*, GAO-11-207 (Washington, D.C.: Dec. 3, 2010).

they arrive at U.S. ports and assess risks based on this information. Among the risk factors considered in assessing each vessel and crew member are whether the vessel operator has had past instances of invalid or incorrect crew manifest lists, whether the vessel has a history of seafarers unlawfully landing in the United States, or whether the vessel is making its first arrival at a U.S. seaport within the past year. The Coast Guard may also conduct armed security boardings of arriving commercial vessels based on various factors, including the intelligence it received to examine crew passports and visas, among other things, to ensure the submitted crew lists are accurate.

- **Conducting vessel escorts and boardings:** The Coast Guard escorts and boards certain vessels to help ensure their security. The Coast Guard escorts a certain percentage of high capacity passenger vessels—cruise ships, ferries, and excursion vessels—to protect against an external threat, such as a waterborne improvised explosive device. The Coast Guard has provided escorts for cruise ships to help prevent waterside attacks and has also provided a security presence on passenger ferries during their transit. Further, the Coast Guard has conducted energy commodity tanker security activities, such as security boardings, escorts, and patrols. Such actions enhance the security of these vessels.

Maritime Domain Awareness and Information Sharing

DHS has worked with its component agencies to increase maritime domain awareness and taken steps to (1) conduct risk assessments, (2) establish area security committees, (3) implement a vessel tracking system, and (4) better share information with other law enforcement agencies through interagency operations centers.

- **Conducting risk assessments:** Recognizing the shortcomings of its existing risk-based models, in 2005 the Coast Guard developed and implemented the Maritime Security Risk Assessment Model (MSRAM) to better assess risks in the maritime domain. We reported in November 2011 that MSRAM provides the Coast Guard with a standardized way of assessing risk to maritime infrastructure, such as chemical facilities, oil refineries, and ferry and cruise ship terminals, among others. Coast Guard units throughout the country use this

model to improve maritime domain awareness and better assess security risks to key maritime infrastructure.²²

- **Establishing Area Maritime Security Committees:** To facilitate information sharing with port partners and in response to MTSA,²³ the Coast Guard has established Area Maritime Security Committees. These committees are typically composed of members from federal, state, and local law enforcement agencies; maritime industry and labor organizations; and other port stakeholders that may be affected by security policies. An Area Maritime Security Committee is responsible for, among other things, identifying critical infrastructure and operations, identifying risks, and providing advice to the Coast Guard for developing the associated AMSP. These committees provide a structure that improves information sharing among port stakeholders.
- **Developing vessel tracking systems:** The Coast Guard relies on a diverse array of systems operated by various entities to track vessels and provide maritime domain awareness. For tracking vessels at sea, the Coast Guard uses a long-range identification and tracking system and a commercially provided long-range automatic identification system.²⁴ For tracking vessels in U.S. coastal areas, inland waterways, and ports, the Coast Guard operates a land-based automatic identification system and also obtains information from radar and cameras in some ports. In addition, in July 2011, CBP developed the Small Vessel Reporting System to better track small boats arriving from foreign locations and deployed this system to eight field locations. Among other things, this system is to allow CBP to

²²GAO, *Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*, GAO-12-14 (Washington, D.C.: Nov. 17, 2011).

²³ 46 U.S.C. § 70112(a)(2).

²⁴The International Maritime Organization is the international body responsible for improving maritime safety. The organization primarily regulates maritime safety and security through the International Convention for the Safety of Life at Sea, 1974. In 2006, amendments to this treaty were adopted that mandated the creation of an international long-range identification and tracking system that, in general, requires the International Maritime Organization member state vessels on international voyages to transmit certain information; the creation of data centers that will, among other roles, receive long-range identification and tracking system information from the vessels; and an information exchange network, centered on an international data exchange for receiving and transmitting long-range identification and tracking information to authorized nations.

identify potential high-risk small boats to better determine which need to be boarded.

- Establishing interagency operations centers:** DHS and its component agencies have made limited progress in establishing interagency operations centers. The Coast Guard—in coordination with other federal, state, and local law enforcement agencies (port partners)—is working to establish interagency operations centers at its sectors throughout the country. These interagency operations centers are designed to, among other things, improve maritime domain awareness and the sharing of information among port partners. In October 2007, we reported that the Coast Guard was piloting various aspects of future interagency operations centers at its 35 existing command centers and working with multiple interagency partners to further their development.²⁵ We further reported in February 2012 that DHS had also begun to support efforts to increase port partner participation and further interagency operations center implementation, such as facilitating the review of an interagency operations center management directive.²⁶ However, as discussed later in this statement, despite the DHS assistance, the Coast Guard has experienced coordination challenges that have limited implementation of interagency operations centers.

International Supply Chain Security

DHS and its component agencies have implemented a number of programs and activities intended to improve the security of the international supply chain, including: enhancing cargo screening and inspections, deploying new cargo screening technologies to better detect contraband, implementing programs to inspect U.S.-bound cargo at foreign ports, partnering with the trade industry, and engaging with international partners.

- Enhancing cargo screening and inspections:** DHS has implemented several programs to enhance the screening of cargo containers in advance of their arrival in the United States. In particular, DHS developed a system for screening incoming cargo, called the Automated Targeting System. The Automated Targeting

²⁵GAO-08-126T.

²⁶GAO, *Maritime Security: Coast Guard Needs to Improve Use and Management of Interagency Operations Centers*, GAO-12-202 (Washington, D.C.: Feb. 13, 2012).

System is a computerized system that assesses information on each cargo shipment that is to arrive in the United States to assign a risk score. CBP officers then use this risk score, along with other information, such as the shipment's contents, to determine which shipments to examine. In February 2003, CBP began enforcing new regulations about cargo manifests—called the 24 hour rule—that requires the submission of complete and accurate manifest information 24 hours before a container is loaded onto a U.S.-bound vessel at a foreign port. To enhance CBP's ability to target high-risk shipments, the SAFE Port Act required CBP to collect additional information related to the movement of cargo to better identify high-risk cargo for inspection.²⁷ In response to this requirement, in 2009, CBP implemented the Importer Security Filing and Additional Carrier Requirements, collectively known as the 10+2 rule.²⁸ The cargo information required by the 10+2 rule comprises 10 data elements from importers, such as country of origin, and 2 data elements from vessel carriers, such as the position of each container transported on a vessel (or stow plan), that are to be provided to CBP in advance of arrival of a shipment at a U.S. port. These additional data elements can enhance maritime security. For example, during our review of CBP's supply chain security efforts in 2010, CBP officials stated that access to vessel stow plans has enhanced their ability to identify containers that are not correctly listed on manifests that could potentially pose a security risk in that no information is known about their origin or contents.²⁹

- **Deploying technologies:** DHS technological improvements have been focused on developing and deploying equipment to scan cargo containers for nuclear materials and other contraband to better secure the supply chain. Specifically, to detect nuclear materials, CBP, in coordination with DNDO, has deployed over 1,400 radiation portal

²⁷See 6 U.S.C. § 943(b).

²⁸Importer Security Filing and Additional Carrier Requirements, 73 Fed. Reg. 71,730 (Nov. 25, 2008) (codified at 19 C.F.R. pts. 4, 12, 18, 101, 103, 113, 122, 123, 141, 143, 149, 178, & 192).

²⁹GAO, *Supply Chain Security: CBP Has Made Progress in Assisting the Trade Industry in Implementing the New Importer Security Filing Requirements, but Some Challenges Remain*, GAO-10-841 (Washington, D.C.: Sept. 10, 2010).

monitors at U.S. ports of entry.³⁰ Most of the radiation portal monitors are installed in primary inspection lanes through which nearly all traffic and shipping containers must pass. These monitors alarm when they detect radiation coming from a package, vehicle, or shipping container. CBP then conducts further inspections at its secondary inspection locations to identify the cause of the alarm and determine whether there is a reason for concern.

- **Establishing the Container Security Initiative:** CBP has enhanced the security of U.S.-bound cargo containers through its Container Security Initiative (CSI). CBP launched CSI in January 2002 and the initiative involves partnerships between CBP and foreign customs agencies in select countries to allow for the targeting and examination of U.S.-bound cargo containers before they reach U.S. ports. As part of this initiative, CBP officers use intelligence and automated risk assessment information to identify those U.S.-bound cargo shipments at risk of containing weapons of mass destruction or other terrorist contraband. We reported in January 2008 that through CSI, CBP has placed staff at 58 foreign seaports that, collectively, account for about 86 percent of the container shipments to the United States.³¹ According to CBP officials, the overseas presence of CBP officials has led to more effective information sharing between CBP and host government officials regarding targeting of U.S.-bound shipments.
- **Partnering with the trade industry:** CBP efforts to improve supply chain security include partnering with members of the trade industry. In an effort to strike a balance between the need to secure the international supply chain while also facilitating the flow of legitimate commerce, CBP developed and administers the Customs-Trade Partnership Against Terrorism program. The program is voluntary and 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. For example, participating companies develop security measures and agree to allow CBP to verify, among other things, that their security measures

³⁰Radiation portal monitors are large stationary detectors through which cargo containers and trucks pass as they enter the United States.

³¹GAO, *Supply Chain Security: Examinations of High-Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed*, GAO-08-187 (Washington, D.C.: Jan. 25, 2008).

(1) meet or exceed CBP's minimum security requirements and (2) are actually in place and effective. In return for their participation, members receive benefits, such as a reduced number of inspections or shorter wait times for their cargo shipments. CBP initiated the Customs-Trade Partnership Against Terrorism program in November 2001, and as of November 2010, the most recent date for which we had data, CBP had awarded initial certification—or acceptance of the company's agreement to voluntarily participate in the program³²—to over 10,000 companies.³³ During the course of a company's membership, CBP security specialists observe and validate the company's security practices. Thus, CBP is in a position to identify security changes and improvements that could enhance supply chain security.

- **Achieving mutual recognition arrangements:** CBP has actively engaged with international partners to define and achieve mutual recognition of customs security practices. For example, in June 2007, CBP signed a mutual recognition arrangement with New Zealand—the first such arrangement in the world—to recognize each other's customs-to-business partnership programs, such as CBP's Customs-Trade Partnership Against Terrorism. As of July 2012, CBP had signed six mutual recognition arrangements.³⁴
- **Implementing the International Port Security Program:** Pursuant to MTSA, the Coast Guard implemented the International Port Security Program in April 2004.³⁵ Under this program, the Coast Guard and host nations jointly review the security measures in place at host nations' ports to compare their practices against established security standards, such as the International Maritime Organization's

³²Acceptance occurs after a review of the company's security profile and compliance with customs laws and regulations.

³³Aside from maritime container shippers, members include many top air carriers and freight forwarders.

³⁴CBP has signed mutual recognition arrangements with Canada, the European Union, Japan, Jordan, Korea, and New Zealand.

³⁵ 46 U.S.C. § 70108.

International Ship and Port Facility Security Code.³⁶ 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 at ports worldwide.³⁷ If a country is not in compliance, vessels from that country may be subject to delays before being allowed into the United States. According to Coast Guard documentation, the Coast Guard has visited almost all of the countries that have vessel traffic between them and the United States and attempts to visit countries at least annually to maintain a cooperative relationship.

Challenges Have Hindered Implementation of Maritime Security Programs

DHS and its component agencies have encountered a number of challenges in implementing programs and activities to enhance maritime security since the enactment of MTSA in 2002. In general, these challenges are related to (1) program management and implementation; (2) partnerships and collaboration; (3) resources, funding, and sustainability; and (4) performance measures. Many of our testimonies and reports in the last 10 years have cited these challenges and appendix I summarizes some of the key findings from those products. Examples of challenges in each of these four areas are detailed below.

Program Management and Implementation

DHS and its component agencies have faced program management and implementation challenges in developing MTSA-related security programs, including a lack of adequate planning and internal controls, as well as problems with acquisition programs.

- **Lack of planning:** Given the urgency to take steps to protect the country against terrorism after the September 11, 2001 attacks, some of the actions taken by DHS and its component agencies used an

³⁶The International Port Security Program (ISPS) uses the ISPS Code as the benchmark by which it measures the effectiveness of a country's antiterrorism 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.

³⁷Subsequently, in October 2006, the SAFE Port Act required the Coast Guard to reassess security measures at such foreign ports at least once every 3 years. Pub. L. No. 109-347, § 234, 120 Stat. 1884, 1918-19.

"implement and amend" approach, which has negatively affected the management of some programs. For example, CBP quickly designed and rolled out CSI in January 2002. However, as we reported in July 2003, CBP initially did not have a strategic plan or workforce plan for this security program, which are essential to long-term success and accountability.³⁸ As a result, CBP subsequently had to take actions to address these risks by, for example, developing CSI goals. The Customs-Trade Partnership Against Terrorism program experienced similar problems. For example, when the program was first implemented, CBP lacked a human capital plan. CBP has taken steps to address C-TPAT management and staffing challenges, including implementing a human capital plan.

- **Lack of adequate internal controls:** Several maritime security programs implemented by DHS and its component agencies did not have adequate internal controls. For example, we reported in May 2011 that internal controls over the TWIC program were not designed to provide reasonable assurance that only qualified applicants could acquire the credentials. During covert tests at several selected ports, our investigators were successful in accessing ports using counterfeit credentials and authentic credentials acquired through fraudulent means.³⁹ As a result of our findings, DHS is in the process of assessing internal controls to identify needed corrective actions. In another example, we found that the Coast Guard did not have procedures in place to ensure that its field units conducted security inspections of offshore energy facilities annually in accordance with its guidance.⁴⁰ In response to this finding, the Coast Guard has taken steps to update its inspections database to ensure inspections of offshore facilities are completed.
- **Inadequate acquisitions management:** DHS has also experienced challenges managing some of its acquisition programs. As discussed earlier, CBP coordinated with DNDO to deploy radiation detection

³⁸GAO, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*, GAO-03-770 (Washington, D.C.: July 25, 2003).

³⁹GAO, *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, GAO-11-657 (Washington, D.C.: May 10, 2011).

⁴⁰GAO, *Maritime Security: Coast Guard Should Conduct Required Inspections of Offshore Energy Infrastructure*, GAO-12-37 (Washington, D.C.: Oct. 28, 2011).

monitors at U.S. ports of entry. However, we reported in June 2009 that DHS's cost analysis of one type of device—the advanced spectroscopic portal radiation detection monitors—did not provide a sound analytical basis for DHS's decision to deploy the devices.⁴¹ DNDO officials stated that they planned to update the cost-benefit analysis; however, after spending more than \$200 million on the program, DHS announced, in February 2010, that it was scaling back its plans for development and use of the devices, and subsequently announced, in July 2011, that it was ending the program. DNDO was also involved in developing more advanced nonintrusive inspection equipment—the cargo advanced automated radiography system—in order to better detect nuclear materials that might be heavily shielded. In September 2010 we reported that DNDO was engaged in the research and development phase while simultaneously planning for the acquisition phase and pursued the acquisition and deployment of the radiography machines without fully understanding that the machines would not fit within existing inspection lanes at CBP ports of entry because it had not sufficiently coordinated the operating requirements with CBP.⁴² DHS spent \$113 million on the program and ended up canceling the acquisition and deployment phase of the program in 2007.

Partnerships and Collaboration

DHS has improved how it collaborates with maritime security partners, but challenges in this area remain that stem from issues such as the launch of programs without adequate stakeholder coordination and problems inherent in working with a wide variety of stakeholders.

- **Lack of port partner coordination:** The Coast Guard experienced coordination challenges in developing its information-management and sharing system, called WatchKeeper, which is designed to enhance information sharing with law enforcement agencies and other partners. In particular, we found in February 2012 that the Coast Guard did not systematically solicit input from key federal, state, and local law enforcement agencies that are its port partners at the interagency operations centers, and that port partner involvement in

⁴¹GAO, *Combating Nuclear Smuggling: Lessons Learned from DHS Testing of Advanced Radiation Detection Portal Monitors*, GAO-09-804T (Washington, D.C.: June 25, 2009).

⁴²GAO, *Combating Nuclear Smuggling: Inadequate Communication and Oversight Hampered DHS Efforts to Develop an Advanced Radiography System to Detect Nuclear Materials*, GAO-10-1041T (Washington D.C.: Sept. 15, 2010).

the development of WatchKeeper requirements and the interagency operations center concept was primarily limited to CBP.⁴³ As a result, this lack of port partner input has jeopardized such centers from meeting their intended purpose of improving information sharing and enhancing maritime domain awareness. We reported that the Coast Guard had begun to better coordinate with its port partners to solicit their input on WatchKeeper requirements, but noted that the Coast Guard still faced challenges in getting other port partners to use WatchKeeper as an information sharing tool. We further found that DHS did not initially assist the Coast Guard in encouraging other DHS components to use WatchKeeper to enhance information sharing. However, DHS had increased its involvement in the program so we did not make any recommendations relative to this issue. We did, however, recommend that the Coast Guard implement a more systematic process to solicit and incorporate port partner input to WatchKeeper and the Coast Guard has begun to take actions to address this recommendation. We believe, though, that it is too soon to tell if such efforts will be successful in ensuring that the interagency operations centers serve as more than Coast Guard-centric command and control centers.

- **Challenges in coordinating with multiple levels of stakeholders:** One example of challenges that DHS and its component agencies have faced with state, local, and tribal stakeholders concerns Coast Guard planning for Arctic operations. The Coast Guard's success in implementing an Arctic plan rests in part on how successfully it communicates with key stakeholders—including the more than 200 Alaska native tribal governments and interest groups—but we found in September 2010 that the Coast Guard did not initially share plans with them.⁴⁴ Coast Guard officials told us that they had been focused on communication with congressional and federal stakeholders and intended to share Arctic plans with other stakeholders once plans were determined. DHS agrees that it needs to communicate with additional stakeholders and has taken steps to do so.

⁴³GAO, *Maritime Security: Coast Guard Needs to Improve Use and Management of Interagency Operations Centers*, GAO-12-202 (Washington, D.C.: Feb. 13, 2012).

⁴⁴GAO, *Coast Guard: Efforts to Identify Arctic Requirements Are Ongoing, but More Communication about Agency Planning Efforts Would Be Beneficial*, GAO-10-870 (Washington, D.C.: Sept. 15, 2010).

-
-
- **Difficulties in coordinating with other federal agencies:** DHS has at times experienced challenges coordinating with other federal agencies to enhance maritime security. For example, we reported in September 2010 that federal agencies, including DHS, had collaborated with international and industry partners to counter piracy, but they had not implemented some key practices for enhancing and sustaining collaboration.⁴⁵ Somali pirates have attacked hundreds of ships and taken thousands of hostages since 2007. As Somalia lacks a functioning government and is unable to repress piracy in its waters, the National Security Council—the President's principal arm for coordinating national security policy among government agencies—developed the interagency *Countering Piracy off the Horn of Africa: Partnership and Action Plan (Action Plan)* in December 2008 to prevent, disrupt, and prosecute piracy off the Horn of Africa in collaboration with international and industry partners. According to U.S. and international stakeholders, the U.S. government has shared information with partners for military coordination. However, agencies have made less progress on several key efforts that involve multiple agencies—such as those to address piracy through strategic communications, disrupt pirate finances, and hold pirates accountable—in part because the *Action Plan* does not designate which agencies should lead or carry out 13 of the 14 tasks. We recommended that the National Security Council bolster interagency collaboration and the U.S. contribution to counterpiracy efforts by clarifying agency roles and responsibilities and encouraging the agencies to develop joint guidance to implement their efforts. In March 2011, a National Security Staff official stated that an interagency policy review will examine roles and responsibilities and implementation actions to focus U.S. efforts for the next several years.
 - **Difficulties in coordinating with private sector stakeholders:** In some cases progress has been hindered because of difficulties in coordination with private sector stakeholders. For example, CBP program officials reported in 2010 that having access to Passenger Name Record data for cruise line passengers—such as a passenger's full itinerary, reservation booking date, phone number, and billing information—could offer security benefits similar to those derived from screening airline passengers. However, CBP does not require this

⁴⁵GAO, *Maritime Security: Actions Needed to Assess and Update Plan and Enhance Collaboration among Partners Involved in Countering Piracy off the Horn of Africa*, GAO-10-856 (Washington, D.C.: Sept. 24, 2010).

information from all cruise lines on a systematic basis because CBP officials stated that they would need further knowledge about the cruise lines' connectivity capabilities to estimate the cost to both CBP and the cruise lines to obtain such passenger data. In April 2010, we recommended that CBP conduct a study to determine whether requiring cruise lines to provide automated Passenger Name Record data to CBP on a systematic basis would benefit homeland security.⁴⁶ In July 2011, CBP reported that it had conducted site surveys at three ports of entry to assess the advantage of having cruise line booking data considered in a national targeting process, and had initial discussions with a cruise line association on the feasibility of CBP gaining national access to cruise line booking data.

- Limitations in working with international stakeholders:** DHS and its component agencies face inherent challenges and limitations working with international partners because of sovereignty issues. For example, we reported in July 2010 that sovereignty concerns have limited the Coast Guard's ability to assess the security of foreign ports. In particular, reluctance by some countries to allow the Coast Guard to visit their ports because of concerns over sovereignty was a challenge cited by Coast Guard officials who were trying to complete port visits under the International Port Security Program.⁴⁷ According to the Coast Guard officials, before permitting Coast Guard officials to visit their ports, some countries insisted on visiting and assessing a sample of U.S. ports. Similarly, we reported in April 2005 that CBP had developed a staffing model for CSI to determine staffing needs at foreign ports to implement the program, but was unable to fully staff some ports because of the need for host government permission, among other diplomatic and practical considerations.⁴⁸

Resources, Funding, and Sustainability

Economic constraints, such as declining revenues and increased security costs, have required DHS to make choices about how to allocate its

⁴⁶GAO, *Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain*, GAO-10-400 (Washington, D.C.: Apr. 9, 2010).

⁴⁷GAO, *Maritime Security: DHS Progress and Challenges in Key Areas of Port Security*, GAO-10-940T (Washington, D.C.: July 21, 2010).

⁴⁸GAO, *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).

resources to most effectively address human capital issues and sustain the programs and activities it has implemented to enhance maritime security.

- **Human capital shortfalls:** Human capital issues continue to pose a challenge to maritime security. For example, we reported in November 2011 that Coast Guard officials from 21 of its 35 sectors (60 percent) told us that limited staff time posed a challenge to incorporating MSRAM into strategic, operational, and tactical planning efforts.⁴⁹ Similarly, Coast Guard officials responsible for conducting maritime facility inspections in 4 of the 7 sectors we visited to support our 2008 report on inspections said meeting all mission requirements for which they were responsible was or could be a challenge because of more stringent inspection requirements and a lack of inspectors, among other things. Officials in another sector said available staffing could adequately cover only part of the sector's area of responsibility.⁵⁰
- **Budget and funding constraints:** Budget and funding decisions also affect the implementation of maritime security programs. For example, within the constrained fiscal environment that the federal government is operating, the Coast Guard has had to prioritize its activities and Coast Guard data indicate that some units are not able to meet self-imposed standards related to certain security activities—including boarding and escorting vessels. We reported in October 2007 that this prioritization of activities had also led to a decrease in resources the Coast Guard had available to provide technical assistance to foreign countries to improve their port security.⁵¹ To overcome this, Coast Guard officials have worked with other agencies, such as the Departments of Defense and State, and international organizations, such as the Organization of American States, to secure funding for training and assistance. Further, in the fiscal year 2013 budget, the Coast Guard will have less funding to sustain current assets needed for security missions so that more funds will be available for its top priority—long-term recapitalization of vessels.

⁴⁹GAO-12-14.

⁵⁰GAO-08-12.

⁵¹GAO-08-126T.

Performance Measures

Another challenge that DHS and its component agencies have faced in implementing maritime security-related programs has been the lack of adequate performance measures. In particular, DHS has not always implemented standard practices in performance management.⁵² These practices include, among other things, collecting reliable and accurate data, using data to support missions, and developing outcome measures.

- **Lack of reliable and accurate data:** DHS and its component agencies have experienced challenges collecting complete, accurate, and reliable data. For example, in January 2011 we reported that both CBP and the Coast Guard tracked the frequency of illegal seafarer incidents at U.S. seaports, but the records of these incidents varied considerably among the two component agencies and between the agencies' field and headquarters units.⁵³ As a result, the data DHS used to inform its strategic and tactical plans were of undetermined reliability.⁵⁴ We recommended that CBP and the Coast Guard determine why their data varied and jointly establish a process for sharing and reconciling records of illegal seafarer entries at U.S. seaports. DHS concurred and has made progress in addressing the recommendation. Another example of a lack of reliable or accurate data pertains to the Maritime Information for Safety & Law Enforcement database (MISLE). The MISLE database is the Coast Guard's primary data system for documenting facility inspections and other activities, but flaws in this database have limited the Coast Guard's ability to accurately assess these activities. For example, during the course of our 2011 review of security inspections of offshore energy infrastructure, we found inconsistencies in how offshore facility inspection results and other data were recorded in MISLE.⁵⁵ In July 2011, and partly in response to our review, the Coast

⁵²The standard practices discussed in this statement can be found in GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO-GGD-96-118 (Washington D.C.: June 1996).

⁵³Illegal seafarers include both absconders (a seafarer CBP has ordered detained on board a vessel in port, but who departs a vessel without permission) and deserters (a seafarer CBP grants permission to leave a vessel, but who does not return when required).

⁵⁴GAO, *Maritime Security: Federal Agencies Have Taken Actions to Address Risks Posed by Seafarers, but Efforts Can Be Strengthened*, GAO-11-195 (Washington D.C.: Jan. 14, 2011).

⁵⁵GAO, *Maritime Security: Coast Guard Should Conduct Required Inspections of Offshore Energy Infrastructure*, GAO-12-37 (Washington D.C.: Oct. 28, 2011).

Guard issued new MISLE guidance on documenting the annual security inspections of offshore facilities in MISLE and distributed this guidance to all relevant field units. While this action should improve accountability, the updated guidance does not address all of the limitations we noted with the MISLE database.

- **Not using data to manage programs:** DHS and its component agencies have not always had or used performance information to manage their missions. For example, work we completed in 2008 showed that Coast Guard officials used MISLE to review the results of inspectors' data entries for individual maritime facilities, but the officials did not use the data to evaluate the facility inspection program overall.⁵⁶ We found that a more thorough evaluation of the facility compliance program could provide information on, for example, the variations we identified between Coast Guard units in oversight approaches, the advantages and disadvantages of each approach, and whether some approaches work better than others.
- **Lack of outcome-based performance measures:** DHS and its component agencies have also experienced difficulties developing and using performance measures that focus on outcomes. Outcome-based performance measures describe the intended result of carrying out a program or activity. For example, although CBP had performance measures in place for its Customs-Trade Partnership Against Terrorism program, these measures focused on program participation and facilitating trade and travel and not on improving supply chain security, which is the program's purpose. We recommended in July 2003, March 2005, and April 2008 that CBP develop outcome-based performance measures for this program.⁵⁷ In response to our recommendations, CBP has identified measures to quantify actions required and to gauge Customs-Trade Partnership Against Terrorism's impact on supply chain security. The Coast Guard has faced similar issues with developing and using outcome-based performance measures. For example, we reported in November 2011 that the Coast Guard developed a measure to report its performance

⁵⁶ GAO-08-12.

⁵⁷ See GAO-03-770, *Cargo Security, Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security*, GAO-05-404 (Washington, D.C.: Mar. 11, 2005); and *Supply Chain Security: U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices*, GAO-08-240 (Washington, D.C.: Apr. 25, 2008).

in reducing maritime risk, but faced challenges using this measure to inform decisions.⁵⁸ The Coast Guard has improved the measure to make it more valid and reliable and believes it is a useful proxy measure of performance, but notes that developing outcome-based performance measures is challenging because of limited historical data on maritime terrorist attacks. Given the uncertainties in estimating risk reduction, though, it is unclear if the measure will provide meaningful performance information with which to track progress over time. Similarly, FEMA has experienced difficulties developing outcome-based performance measures. For example, in November 2011 we reported that FEMA was developing performance measures to assess its administration of the Port Security Grant Program, but had not implemented measures to assess the program's grant effectiveness.⁵⁹ FEMA has taken initial steps to develop measures to assess the effectiveness of its grant programs, but it does not have a plan and related milestones for implementing measures specifically for the Port Security Grant Program. Without such performance measures it could be difficult for FEMA to effectively manage the process of assessing whether the program is achieving its stated purpose of strengthening critical maritime infrastructure against risks associated with potential terrorist attacks. We recommended that DHS develop a plan with milestones for implementing performance measures for the Port Security Grant Program. DHS concurred with the recommendation and stated that FEMA is taking actions to implement it.

Mr. Chairman and members of the subcommittee, this completes my prepared statement. I would be happy to respond to any questions you or other members of the subcommittee may have at this time.

⁵⁸GAO-12-14.

⁵⁹GAO-12-47.

Appendix I: Summary of Select Maritime Security-Related Programs and Activities

This appendix provides information on select programs and activities that have been implemented in maritime security since enactment of the Maritime Transportation Security Act (MTSA) in 2002. The information includes an overview of each program or activity; obligations information, where available; a summary of key findings and recommendations from prior GAO work, if applicable; and a list of relevant GAO products.

The Department of Homeland Security (DHS) is the lead federal agency responsible for implementing MTSA requirements and related maritime security programs. DHS relies on a number of its component agencies that have responsibilities related to maritime security, including the following:¹

- **U.S. Coast Guard:** The Coast Guard has primary responsibility for ensuring the safety and security of U.S. maritime interests and leading homeland security efforts in the maritime domain.
- **U.S. Customs and Border Protection (CBP):** CBP is responsible for the maritime screening of incoming commercial cargo for the presence of contraband, such as weapons of mass destruction, illicit drugs, or explosives, while facilitating the flow of legitimate trade and passengers.
- **Transportation Security Administration (TSA):** TSA has responsibility for managing the Transportation Worker Identification Credential (TWIC) program, which is designed to control the access of maritime workers to regulated maritime facilities.²
- **Domestic Nuclear Detection Office (DNDO):** DNDO is responsible for acquiring and supporting the deployment of radiation detection equipment, including radiation portal monitors at U.S. ports of entry.

¹ In addition to the DHS component agencies, the Department of Defense has worked with DHS to draft a National Strategy for Maritime Security and has placed staff at Interagency Operations Centers to coordinate information sharing on maritime security issues with DHS component agencies and other law enforcement agencies. The Department of Energy funds the installation of radiation detection equipment at select seaports overseas through its Megaports Initiative, and the Department of State reviews foreign seafarers' applications for U.S. visas.

² The Coast Guard is responsible for enforcement of the Transportation Worker Identification Credential program.

- **Federal Emergency Management Agency (FEMA):** FEMA is responsible for administering grants to improve the security of the nation's highest risk port areas.

This appendix is based primarily on GAO reports and testimonies issued from August 2002 through July 2012 related to maritime, port, vessel, and cargo security efforts of the federal government, and other aspects of implementing MTSA-related security requirements. The appendix also includes selected updates—conducted in August 2012—to the information provided in these previously-issued products on the actions DHS and its component agencies have taken to address recommendations made in these products and the obligations for key programs and activities through May 2012.

The obligations information provided in this appendix represents obligations for certain maritime security programs and activities that we were able to identify from available agency sources, such as agency congressional budget justifications, budget in brief documents, and prior GAO products.³ It does not represent the total amount obligated for maritime security. In some cases, information was not available because of agency reporting practices. For example, we were not able to determine obligations for many of the MTSA-related Coast Guard programs and activities because they are funded at the account level (i.e., operating expenses) rather than as specific line items.

While we were not able to identify obligations for every maritime security program and activity, many of the Coast Guard's programs and activities in maritime security fall under its ports, waterways, and coastal security mission. Table 1 shows the reported budget authority for the Coast Guard's ports, waterways, and coastal security mission for fiscal years 2004 through 2013. The remainder of the budget-related information contained in this appendix generally pertains to obligations. In several instances we obtained appropriations information when obligations information was not available.

³ The information provided generally reflects agency obligations, unless noted otherwise.

Appendix I: Summary of Select Maritime Security-Related Programs and Activities

Table 1: Ports, Waterways, and Coastal Security Mission's Reported Budget Authority (in millions), Fiscal Years 2004 through 2013

Funding	Fiscal year ^a									
	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
	\$1,853	\$1,638	\$1,760	\$1,362	\$1,554	\$1,641	\$1,598	\$1,651	\$1,918	\$1,738

Source: GAO analysis of Budget in Brief reports.

^aBudget authority data for fiscal year 2003 were not available. Fiscal year 2013 is requested.

National Strategy for Maritime Security

National Strategy for Maritime Security

The *National Strategy for Maritime Security*, published in September 2005, aimed to align all federal government maritime security programs and activities into a comprehensive and cohesive national effort involving appropriate federal, state, local, and private sector entities. Homeland Security Presidential Directive 13 (HSPD-13) directed the Secretaries of Defense and Homeland Security to lead a joint effort to draft a *National Strategy for Maritime Security*.

In addition to the National Strategy, HSPD-13 directed DHS to develop eight supporting implementation plans to address the specific threats and challenges of the maritime environment. While the plans address different aspects of maritime security, they are mutually linked and reinforce each other. The supporting plans are as follows:

- National Plan to Achieve Domain Awareness
- Global Maritime Intelligence Integration Plan
- Interim Maritime Operational Threat Response Plan
- International Outreach and Coordination Strategy
- Maritime Infrastructure Recovery Plan
- Maritime Transportation System Security Plan
- Maritime Commerce Security Plan
- Domestic Outreach Plan

Funding Information

We were unable to obtain funding information for this strategy.

Summary of Key Findings and Recommendations

In June 2008, we reported that the National Strategy for Maritime Security and the supporting plans that implement the strategy show that, collectively, the plans address four of the six desirable characteristics of an effective national strategy that we identified in 2004 and partially address the remaining two. The four characteristics that are addressed include: (1) purpose, scope, and methodology; (2) problem definition and risk assessment; (3) organizational roles, responsibilities, and coordination; and (4) integration and implementation. The two characteristics that are partially addressed are: (1) goals, objectives, activities, and performance measures and (2) resources, investments, and risk management. Specifically, only one of the supporting plans mentions performance measures and many of these measures are presented as possible or potential performance measures. However, in other work reported on in August 2007, we noted the existence of performance measures for individual maritime security programs. These characteristics are partially addressed primarily because the strategy and its plans did not contain information on performance measures and the resources and investments elements of these characteristics. The resources, investments, and risk management characteristic is also partially addressed. While the strategic actions and recommendations discussed in the maritime security strategy and supporting implementation plans constitute an approach to minimizing risk and investing resources, the strategy and seven of its supporting implementation plans did not include information on the sources and types of resources needed for their implementation. In addition, the national strategy and three of the supporting plans also lack investment strategies to direct resources to necessary actions. To address this, the working group tasked with monitoring implementation of the plans recommended that the Maritime Security Policy Coordination Committee—the primary forum for coordinating U.S. national maritime strategy—examine the feasibility of creating an interagency investment strategy for the supporting plans. We recognized that other documents were used for allocating resources and, accordingly, we did not make any recommendations.

Relevant GAO Products

Maritime Security: Coast Guard Efforts to Address Port Recovery and Salvage Response. GAO-12-494R. Washington, D.C.: April 6, 2012. See page 4.

National Strategy and Supporting Plans Were Generally Well-Developed and Are Being Implemented. GAO-08-672. Washington, D.C.: June 20, 2008.

Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions. GAO-07-454. Washington, D.C.: August 17, 2007. See pages 108-109.

Area Maritime Security Plans

Area Maritime Security Plans

Area Maritime Security Plans (AMSPs) are developed by the Coast Guard with input from applicable governmental and private entities and these plans serve as the primary means to identify and coordinate Coast Guard procedures related to prevention, protection, and security response. Among other requirements, MTTSA directed the Coast Guard to develop AMSPs—to be updated every 5 years—for ports throughout the nation (46 U.S.C. § 70103(b)(2)(G)). AMSPs are developed for each of 43 geographically defined port areas. In 2006, the Security and Accountability for Every Port Act (SAFE Port Act) added a requirement that AMSPs include recovery issues by identifying salvage equipment able to restore operational trade capacity (46 U.S.C. § 70103(b)(2)(G)).

Budget Authority Information

Activities related to AMSPs are not specifically identified in the Coast Guard budget. Such activities fall under the Coast Guard's ports, waterways and coastal security mission. See table 1 for the reported budget authority for that mission for fiscal years 2004 through 2013.

Summary of Key Findings and Recommendations

Our work on AMSP showed progress and an evolution toward plans that were focused on preventing terrorism and included discussion regarding natural disasters with detailed information on plans for recovery after an incident. We reported in October 2007 that the Coast Guard developed guidance and a template to help ensure that all major ports had an original AMSP that was to be updated every 5 years. Our 2007 reports stated that there was a wide variance in ports' natural disaster planning efforts and that AMSPs—limited to security incidents—could benefit from unified planning to include an all-hazards approach. In our March 2007 report on this issue, we recommended that DHS encourage port stakeholders to use existing forums for discussing all-hazards planning. The Coast Guard's early attempts to set out the general priorities for recovery operations in its guidelines for the development of AMSPs offered limited instruction and assistance for developing procedures to address recovery situations. Our April 2012 report stated that each of the seven Coast Guard AMSPs that we reviewed had incorporated key recovery and salvage response planning elements as called for by legislation and Coast Guard guidance.¹ Specifically, the plans included the roles and responsibilities of special recovery units, instructions for gathering key information on the status of maritime assets (such as bridges), identification of recovery priorities, and plans for salvage of assets following an incident.

Relevant GAO Products

Maritime Security: Coast Guard Efforts to Address Port Recovery and Salvage Response. GAO-12-494R. Washington, D.C.: April 6, 2012.

The SAFE Port Act: Status and Implementation One Year Later. GAO-08-126T. Washington, D.C.: October 30, 2007. Pages 12-14.

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

¹ See 46 U.S.C. § 70103(b)(2)(E), (G).

Port Security Exercises

Port Security Exercises

Port Security Exercises are designed to continuously improve preparedness by validating information and procedures in the AMSPs, identifying strengths and weaknesses, and practicing command and control within an incident command/unified command framework. The Coast Guard Captain of the Port—the port officer designated to enforce, among other things, port security—and the Area Maritime Security Committee—a committee of key port stakeholders who share information and develop port security plans—are required by Coast Guard regulations to conduct or participate in exercises to test the effectiveness of AMSPs annually, with no more than 18 months between exercises (33 C.F.R. § 103.515). After these exercises are conducted, the Coast Guard requires that the units participating in the exercise submit an after-action report describing the results and highlighting any lessons learned.

In August 2005, the Coast Guard and TSA initiated the Port Security Training Exercise Program. Additionally, the Coast Guard initiated its own Area Maritime Security Training and Exercise Program in October 2005. Both programs were designed to involve the entire port community in exercises. In 2006, the SAFE Port Act included several new requirements related to security exercises, such as establishing a Port Security Exercise Program and an improvement plan process that would identify, disseminate, and monitor the implementation of lessons learned and best practices from port security exercises (6 U.S.C. § 912).

Budget Authority Information

Activities related to port security exercises are not specifically identified in the Coast Guard budget. Such activities fall under the Coast Guard's ports, waterways and coastal security mission. See table 1 for the reported budget authority for that mission for fiscal years 2004 through 2013.

Summary of Key Findings and Recommendations

In January 2005, we reported that the Coast Guard had conducted many exercises and was successful in identifying areas for improvement—which is the purpose of such exercises. For example, Coast Guard port security exercises identified opportunities to improve incident response in the areas of communication, resources, coordination, and decision-making authority. Further, we reported that after-action reports were not being completed in a timely manner. We recommended that the Coast Guard review its actions for ensuring the timely submission of after-action reports on terrorism-related exercises and determine if further actions are needed. To address the issue of timeliness, the Coast Guard reduced the timeframe allowed for submitting an after-action report. All reports are now required to be reviewed, validated, and entered into the applicable database within 21 days of the end of an exercise or operation. In addition, our analysis of 26 after-action reports for calendar year 2006 showed an improvement in the quality of these reports in that each report listed specific exercise objectives and lessons learned. As a result of these improvements in meeting requirements for after action reports, the Coast Guard is in a better position to identify and correct barriers to a successful response to a terrorist threat. Our October 2011 report on offshore energy infrastructure stated that the Coast Guard had conducted exercises and taken corrective actions, as appropriate, to strengthen its ability to prevent a terrorist attack on an offshore facility. This included a national-level exercise that focused on, among other things, protecting offshore facilities in the Gulf of Mexico. The exercise resulted in more than 100 after-action items and, according to Coast Guard documentation, the Coast Guard had taken steps to resolve the majority of them and was working on the others.

Relevant GAO Products

Maritime Security: Coast Guard Should Conduct Required Inspections of Offshore Energy Infrastructure. GAO-12-37. Washington, D.C.: October 28, 2011. See pages 17-18 and 48-49.

The SAFE Port Act: Status and Implementation One Year Later. GAO-08-126T. Washington, D.C.: October 30, 2007. See pages 14-15.

Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention. GAO-05-170, January 14, 2004.

Maritime Facility Security Plans

Maritime Facility Security Plans

MTSA requires various types of maritime facilities to develop and implement security plans and it places federal responsibility for approving and overseeing these plans with DHS (46 U.S.C. § 70103(c)). DHS, in turn, has delegated this administrative responsibility to the Coast Guard. The SAFE Port Act, enacted in 2006, requires the Coast Guard to conduct at least two inspections of each maritime facility annually—one of which is to be unannounced—to verify continued compliance with each facility's security plan (46 U.S.C. § 70103(c)(4)(D)). As of June 2004, approximately 3,150 facilities were required to develop facility security plans.

Budget Authority Information

Activities related to maritime facility security plans are not specifically identified in the Coast Guard budget. Such activities fall under the Coast Guard's ports, waterways and coastal security mission. See table 1 for the reported budget authority for that mission for fiscal years 2004 through 2013.

Summary of Key Findings and Recommendations

Our work on this issue found that the Coast Guard has made progress by generally requiring maritime facilities to develop security plans and conducting required annual inspections. We also reported that the Coast Guard's inspections were identifying and correcting facility deficiencies. For example, in February 2008, we reported that the Coast Guard identified deficiencies in about one-third of the facilities inspected from 2004 through 2006, with deficiencies concentrated in certain categories, such as failing to follow facility security plans for access control. Our work also found areas for improvement as well. For example, in February 2008 we made recommendations to help ensure effective implementation of MTSA-required facility inspections. For example, we recommended that the Coast Guard reassess the number of inspections staff needed, among other things. In response, the Coast Guard took action to implement these recommendations. In our October 2011 report on inspections of offshore energy facilities, we noted that the Coast Guard had taken actions to help ensure the security of offshore energy facilities, such as developing and reviewing security plans, but faced difficulties ensuring that all facilities complied with requirements. We recommended that the Coast Guard develop policies or guidance to ensure that annual security inspections are conducted and information entered into databases is more useful for management. The Coast Guard concurred with these recommendations and stated that it plans to update its guidance and improve its inspection database in 2013.

Relevant GAO Products

Maritime Security: Coast Guard Should Conduct Required Inspections of Offshore Energy Infrastructure. GAO-12-37. Washington, D.C.: October 28, 2011.

Maritime Security: The SAFE Port Act: Status and Implementation One Year Later. GAO-08-126T. Washington D.C.: October 30, 2007. See pages 19-21.

Maritime Security: Coast Guard Inspections Identify and Correct Facility Deficiencies, but More Analysis Needed of Program's Staffing, Practices, and Data. GAO-08-12. Washington D.C.: February 14, 2008.

Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions. GAO-07-454. Washington D.C.: August 17, 2007. See page 110.

Maritime Security: Substantial Work Remains to Translate New Planning Requirements to Effective Port Security. GAO-04-838. Washington, D.C.: June 30, 2004.

Port Security Grant Program

Port Security Grant Program

The Port Security Grant Program (PSGP) provides federal funding to defray some of the costs of implementing security measures at domestic ports. The program was established in January 2002 and codified by MTA (46 U.S.C. § 70107). DHS administers the PSGP through the Federal Emergency Management Agency (FEMA), and the Coast Guard provides subject matter expertise to FEMA on the maritime industry to inform grant award decisions.

Based on risk, each port is placed into one of three funding groups—Group I (highest risk group), Group II (next highest risk group), or Group III. Port areas not identified in these groups are eligible to apply for funding as part of the "All Other Port Areas" Group. Port areas use PSGP funding to increase portwide risk management, enhance maritime domain awareness, and improve port recovery and resiliency efforts through developing security plans, purchasing security equipment, and providing security training to employees.

Table 2: Total PSGP Funding^a Fiscal Year 2003 through 2012 (in millions)

PSGP	Fiscal year									
	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Funding amount	244 ^b	179	141	168	311 ^c	389	389	288	235	97.5
Total for all years	\$2,441.5d									

Source: FEMA's annual PSGP grant guidance and GAO analysis of DHS appropriations

^aTarget funding amounts as presented in FEMA's annual grant guidance.

^bThis figure includes \$169 million in PSGP funding and \$75 million in additional funding for port security under the Urban Areas Security Initiative—another DHS grant program that provides funding for building and sustaining national preparedness capabilities.

^cThis figure includes fiscal year 2007 appropriations, as well as \$110 million in fiscal year 2007 supplemental appropriation.

^dTotal funding includes totals through fiscal year 2012, as well as \$150 million provided pursuant to the American Recovery and Reinvestment Act (ARRA). Pub. L. No. 111-5, 123 Stat. 145, 164 (2009).

Summary of Key Findings and Recommendations

We reported in November 2011 that the PSGP is one of DHS's tools to protect critical maritime infrastructure from risks such as terrorist attacks. Consistent with risk management principles, in November 2011, we also reported that PSGP allocations were highly correlated to risk and DHS has taken steps to strengthen the PSGP risk allocation model by improving the quality and precision of the data inputs. However, since fiscal year 2006, we have also reported that DHS did not have measures to assess the programs' effectiveness and recommended that DHS develop performance measures. In November 2011, we reported that DHS was not in the best position to monitor the program's effectiveness and recommended that FEMA establish time frames and related milestones for implementing performance measures. We also recommended that FEMA update the PSGP risk model to incorporate variability in port vulnerabilities. DHS concurred with our recommendations and is taking steps to address them. For example, DHS officials stated that FEMA is in the process of developing performance measures.

Relevant GAO Products

Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened. GAO-12-47. Washington, D.C.: November 17, 2011.

Maritime Security: Responses to Questions for the Record. GAO-11-140R. Washington D.C.: October 22, 2010. See pages 12-15.

Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure. GAO-06-91. Washington, D.C.: December 15, 2005. See pages 49-67.

Transportation Worker Identification Credential

Transportation Worker Identification Credential

The Transportation Worker Identification Credential (TWIC) program, administered by the Coast Guard and TSA, requires maritime workers to complete background checks and obtain a biometric identification card to gain unescorted access to secure areas of regulated maritime facilities.

MTSA required the Secretary of Homeland Security to prescribe regulations preventing individuals from having unescorted access to secure areas of MTSA-regulated facilities unless they possess a biometric transportation security card and are authorized to be in such an area. It also tasked DHS with the responsibility to issue identification cards to eligible individuals.

According to the most recently available data from the Coast Guard, as of December 2010 and January 2011, there were 2,509 facilities and 12,908 vessels, respectively, that were subject to MTSA regulations and had to implement TWIC provisions. According to TSA, as of August 9, 2012, it has activated over 2 million TWIC cards.

Table 3: Total TWIC Funding Authority, Fiscal Years 2003 through June 2012 (in millions)

TWIC	Fiscal year										
	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	
Funding authority ^a	25.0	49.7	5.0	15.0	18.6	50.6	109.3	45.0	45.0	30.2	
Total for all years											\$393.4

Source: GAO analysis of TWIC program funding reported by TSA and FEMA.

^aFunding authority includes appropriations with reprogramming and adjustments and TWIC fee authority. TWIC fee authority represent the dollar amount TSA is authorized to collect from TWIC enrollment fees and not the actual dollars collected. TSA reports it has collected \$41.7 million for fiscal year 2008, \$76.2 million for fiscal year 2009, \$30.6 million for fiscal year 2010, \$26.5 million for fiscal year 2011, and \$21.1 million for fiscal year 2012 (as of June 30). The total does not include \$151 million in FEMA security grant funding.

Summary of Key Findings and Recommendations

Our work on TWIC has shown that DHS, TSA, and the Coast Guard have made progress in enrolling workers and activating TWICs. For example, in November 2009, we reported that over 93 percent of the estimated TWIC users were enrolled in the program by the April 15, 2009 compliance deadline. However, TSA, the Coast Guard, and maritime industry stakeholders have faced challenges in implementing the TWIC program. These challenges include enrolling and issuing TWICs to a larger population than was originally anticipated, ensuring that TWIC access control technologies perform effectively in the harsh maritime environment, and balancing security requirements with the need to facilitate the flow of legitimate maritime commerce. We have recommended that DHS take actions to identify effective and cost-efficient methods for meeting TWIC program objectives and evaluate those actions. In general DHS concurred with our recommendations and has plans underway to implement them. In addition, as mandated by the Coast Guard Authorization Act of 2010,² we are currently assessing the results of the TWIC pilot and will report on our findings later this year.

Relevant GAO Products

Transportation Worker Identification Credential: Internal Control Weaknesses Need to be Corrected to Help Achieve Security Objectives. GAO-11-657. Washington, D.C.: May 10, 2011.

Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers. GAO-10-43. Washington, D.C.: November 18, 2009.

² Pub. L. No. 111-281, § 802, 124 Stat. 2905, 2999 (2010).

Vessel Security Plans

Vessel Security Plans

Coast Guard regulations require owners and operators of certain vessels to conduct assessments to identify security vulnerabilities, and to develop plans to mitigate these vulnerabilities (33 C.F.R. §§ 104.300-415). The Coast Guard set a deadline for vessels to operate under an approved or self-certified security plan by July 1, 2004. The U.S. Coast Guard was responsible for (1) determining which vessels are required to create these plans and (2) reviewing and approving the vessel security plans.

According to the Coast Guard, as of June 2004 there were almost 10,000 vessels operating in more than 300 domestic ports that were required to comply with these MTSA requirements. These maritime vessels, ranging from oil tankers and freighters to tugboats and passenger ferries, can be vulnerable on many security-related fronts and, therefore, must be able to restrict access to areas on board, such as the pilot house or other control stations critical to the vessels' operation.

The effect of the Coast Guard's oversight of vessel security plans extends far beyond U.S. waters to high risk areas—such as the Horn of Africa—where piracy has surged in the last few years. For example, the Coast Guard ensures that the more than 100 U.S.-flagged vessels that travel through that region have updated security plans, and the Coast Guard checks for compliance when these vessels are at certain ports.

Budget Authority Information

Activities related to vessel security plans are not specifically identified in the Coast Guard budget. Such activities fall under the Coast Guard's ports, waterways and coastal security mission. See table 1 for the reported budget authority for that mission for fiscal years 2004 through 2013.

Summary of Key Findings and Recommendations

We reported in June 2004 that the Coast Guard had identified and corrected deficiencies in vessel security plans, though the extent of review and approval of such plans varied widely. Our more recent vessel security work has focused on specific types of vessels—including ferries, cruise ships, and energy commodity tankers—and found that the Coast Guard has taken a number of steps to improve their security, such as screening vehicles and passengers on ferries. Our September 2010 report on piracy found that the Coast Guard had ensured that the security plans for U.S.-flagged vessels have been updated with piracy annexes if they transited high risk areas. Our work has also identified additional opportunities to enhance vessel security. For example, in 2010 we reported that the Coast Guard had not implemented recommendations from five agency contracted studies on ferry security and that the Coast Guard faced challenges protecting energy tankers. We made recommendations aimed at increasing security aboard vessels. In general DHS has concurred with these recommendations and is in the process of implementing them.

Relevant GAO Products

Maritime Security: Ferry Security Measures Have Been Implemented, but Evaluating Existing Studies Could Further Enhance Security. GAO-11-207. Washington D.C.: December 3, 2010.

Maritime Security: Actions Needed to Assess and Update Plan and Enhance Collaboration Among Partners Involved in Countering Piracy off the Horn of Africa. GAO-10-856. Washington D.C.: September 30, 2010. See pages 57-59.

Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain. GAO-10-400. Washington, D.C.: April 9, 2010.

Maritime Security: Federal Efforts Needed to Address Challenges in Preventing and Responding to Terrorist Attacks on Energy Commodity Tankers. GAO-08-141. Washington, D.C.: December 10, 2007.

Maritime Security: Substantial Work Remains to Translate New Planning Requirements to Effective Port Security. GAO-04-838. Washington, D.C.: June 30, 2004.

Small Vessel Security Activities

Small Vessel Security Activities

Small vessel security activities are those in place to address the threat posed by the millions of small vessels in use in U.S. waterways. Related to this threat, DHS released its *Small Vessel Security Strategy* in April 2008 as part of its effort to mitigate the vulnerability of vessels to waterside attacks from small vessels. As part of the Strategy, DHS identified the four gravest risk scenarios involving the use of small vessels for terrorist attacks—(1) a waterborne improvised explosive device, (2) a means of smuggling weapons into the United States, (3) a means of smuggling humans into the United States, and (4) a platform for conducting an attack that uses a rocket or other weapon launched at a sufficient distance to allow the attackers to evade defensive fire.

Budget Authority Information

Activities related to small vessel security activities are not specifically identified in the Coast Guard budget. Such activities fall under the Coast Guard's ports, waterways and coastal security mission. See table 1 for the reported budget authority for that mission for fiscal years 2004 through 2013.

Summary of Key Findings and Recommendations

We reported in October 2010 that DHS—including the Coast Guard and CBP—and other entities are taking actions to reduce the risk from small vessels attacks. These actions include the development of the *Small Vessel Security Strategy*, community outreach, the establishment of security zones in U.S. ports and waterways, escorts of vessels that could be targeted for attack and port-level vessel tracking with radars and cameras since other vessel tracking systems—such as the Automatic Identification System—are only required on larger vessels. Our October 2010 work indicates, however, that the expansion of vessel tracking to all small vessels may be of limited utility because of, among other things, the large number of small vessels, the difficulty identifying threatening actions, and the challenges associated with getting resources on scene in time to prevent an attack once it has been identified. To enhance actions to address the small vessel threat DNDO has worked with the Coast Guard and local ports to develop and test equipment for detecting nuclear material on small maritime vessels. As part of our broader work on DNDO's nuclear detection architecture, in January 2009 we recommended that DNDO develop a comprehensive plan for installing radiation detection equipment that would define how DNDO would achieve and monitor its goal of detecting the movement of radiological and nuclear materials through potential smuggling routes, such as small maritime vessels. DHS generally concurred with the recommendation and is in the process of implementing it.

Relevant GAO Products

Maritime Security: DHS Progress and Challenges in Key Areas of Port Security. GAO-10-940T. Washington, D.C.: July 21, 2010. See pages 7-10.

Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed. GAO-09-337. Washington, D.C.: March 17, 2009. See pages 30-37.

Nuclear Detection: Domestic Nuclear Detection Office Should Improve Planning to Better Address Gaps and Vulnerabilities. GAO-09-257. Washington, D.C.: January 29, 2009. See pages 18-23.

Nuclear Detection: Preliminary Observations on the Domestic Nuclear Detection Office's Efforts to Develop a Global Nuclear Detection Architecture. GAO-08-999T. Washington, D.C.: July 16, 2008.

Controls over Foreign Seafarers

Controls over Foreign Seafarers

In fiscal year 2009, maritime crew—known as seafarers—made about 5 million entries into U.S. ports on commercial cargo and cruise ship vessels. This is important because the overwhelming majority of seafarers on arriving vessels are aliens. Because the U.S. government has no control over foreign seafarer credentialing practices, concerns have been raised that it is possible for aliens to fraudulently obtain seafarer credentials to gain entry into the United States or conduct attacks. Therefore, DHS considers the illegal entry of an alien through a U.S. seaport through exploitation of maritime industry practices to be a key concern. Within DHS, the Coast Guard and CBP conduct a variety of seafarer-related enforcement and compliance boardings and inspections. For example, the Coast Guard conducts inspections of vessel crew as part of its regulatory responsibility under MTTSA. Other departments participate as well, such as the State Department, which reviews foreign seafarers' applications for U.S. visas.

A few countries account for a large share of arriving foreign seafarers, with the Philippines, India, and Russia supplying the most. According to the Coast Guard, approximately 80 percent of seafarers arriving by commercial vessel did so aboard passenger vessels, such as cruise ships.

Budget Authority Information

Activities related to controls over foreign seafarers are not specifically identified in the Coast Guard budget. Some of these fall under the Coast Guard's ports, waterways and coastal security mission. See table 1 for the reported budget authority amounts for that mission for fiscal years 2004 through 2013.

Summary of Key Findings and Recommendations

We reported in January 2011 that the federal government uses a multi-faceted strategy to address foreign seafarer risks. The State Department starts the process by reviewing seafarer applications for U.S. visas. As part of this process, consular officers review applications, interview applicants, screen applicant information against federal databases, and review supporting documents to assess whether the applicants pose a potential threat to national security, among other things. In addition, DHS and its component agencies conduct advance-screening inspections, assess risks, and screen seafarers. However, our work noted opportunities to enhance seafarer inspection methods. For example, in January 2011, we reported that CBP inspected all seafarers entering the United States, but noted that CBP did not have the technology to electronically verify the identity and immigration status of crews on board cargo vessels, thus limiting CBP's ability to ensure it could identify fraudulent documents presented by foreign seafarers. We made several recommendations to, among other things, facilitate better understanding of the potential need and feasibility of expanding electronic verification of seafarers on board vessels and to improve data collection and sharing. In that same report we also noted discrepancies between CBP and Coast Guard data on illegal seafarer entries at domestic ports and we recommended that the two agencies jointly establish a process for sharing and reconciling such records. DHS concurred with our recommendations and is in the process of taking actions to implement them. For example, CBP met with the DHS Screening Coordination Office to determine risks associated with not electronically verifying foreign seafarers for admissibility. Further, DHS reported in July 2011 that CBP and the Coast Guard were working to assess the costs associated with deploying equipment to provide biometric reading capabilities on board vessels.

Relevant GAO Product

Maritime Security: Federal Agencies Have Taken Actions to Address Risks Posed by Seafarers, but Efforts Can Be Strengthened. GAO-11-195. Washington, D.C.: January 14, 2011.

Maritime Security Risk Analysis Model

Maritime Security Risk Analysis Model

The Maritime Security Risk Analysis Model (MSRAM) is the Coast Guard's primary tool for assessing and managing security risks in the maritime domain. The Coast Guard uses MSRAM to meet DHS's requirement for using risk-informed approaches to prioritize its investments.

MSRAM provides the Coast Guard with a standardized way of assessing risk to maritime infrastructure, such as chemical facilities, oil refineries, hazardous cargo vessels, passenger ferries, and cruise ship terminals, among others. MSRAM calculates the risk of a terrorist attack based on scenarios—a combination of target and attack modes—in terms of threats, vulnerabilities, and consequences to more than 28,000 maritime targets. The model focuses on individual facilities and cannot model system impacts or more complex scenarios involving adaptive or intelligent adversaries. The Coast Guard also uses MSRAM as input into other DHS maritime security programs, such as FEMA's Port Security Grant Program.

The Coast Guard Authorization Act of 2010 required the Coast Guard to make MSRAM available, in an unclassified version, on a limited basis to regulated vessels and facilities to conduct risk assessments of their own facilities and vessels (Pub. L. No. 111-281, § 827, 124 Stat. 2905, 3004-05).

Budget Authority Information

Activities related to MSRAM are not specifically identified in the Coast Guard budget. Such activities fall under the Coast Guard's ports, waterways and coastal security mission. See table 1 for the reported budget authority for that mission for fiscal years 2004 through 2013.

Summary of Key Findings and Recommendations

Our work on MSRAM found that the Coast Guard's risk management and risk assessment efforts have developed and evolved and that the Coast Guard has made progress in assessing maritime security risks using MSRAM. For example, our work in this area in 2005 found that the Coast Guard was ahead of other DHS components in establishing a foundation for using risk management. After the September 11, 2001 terrorist attacks, the Coast Guard greatly expanded the scope of its risk assessment activities. It conducted three major security assessments at ports, which collectively resulted in progress in understanding and prioritizing risks within a port. We also reported in July 2010 that by developing MSRAM, the Coast Guard had begun to address the limitations of its previous port security risk model. In our more recent work, we reported that MSRAM generally aligns with DHS risk assessment criteria, but noted that additional documentation and training could benefit MSRAM users. We made recommendations to the Coast Guard to strengthen MSRAM, better align it with risk management guidance, and facilitate its increased use across the agency. In general, the Coast Guard has concurred with our recommendations and has implemented some and taken actions to implement others. For example, the Coast Guard uses risk management to drive resource allocations across its missions and is in the process of making MSRAM available for external peer review. The Coast Guard expects to complete these actions later this year.

Relevant GAO Products

Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations. GAO-12-14. Washington, D.C.: November 17, 2011.

Maritime Security: DHS Progress and Challenges in Key Areas of Port Security. GAO-10-940T. Washington, D.C.: July 21, 2010. See pages 3-6.

Risk Management: Further Refinements Needed To Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure. GAO-06-91. Washington, D.C.: December 15, 2005. See pages 30-48.

Area Maritime Security Committees

Area Maritime Security Committees

Area Maritime Security Committees (AMSCs) consist of key stakeholders who (1) may be affected by security policies and (2) share information and develop port security plans. AMSCs, which are required by Coast Guard regulations that implement MTSA, also identify critical port infrastructure and risks to the port, develop mitigation strategies for these risks, and communicate appropriate security information to port stakeholders (33 C.F.R. §§ 103.300-310). AMSCs were created, in part, because ports are sprawling enterprises that often cross jurisdictional boundaries; and the need to share information among federal, state and local agencies is central to effective prevention and response.

According to the Coast Guard, it has organized 43 area maritime security committees, covering the nation's 361 ports. Recommended members of AMSCs are a diverse array of port stakeholders to include federal, state and local agencies, as well as private sector entities to include terminal operators, yacht clubs, shipyards, marine exchanges, commercial fishermen, trucking and railroad companies, organized labor, and trade associations.

Budget Authority Information

Activities related to AMSCs are not specifically identified in the Coast Guard budget. Such activities fall under the Coast Guard's ports, waterways and coastal security mission. See table 1 for the reported budget authority for that mission for fiscal years 2004 through 2013.

Summary of Key Findings and Recommendations

Our work in this area has noted that the Coast Guard has established AMSCs in major U.S. ports. We also reported in April 2005 that the AMSCs improved information sharing among port stakeholders, and made improvements in the timeliness, completeness, and usefulness of such information. The types of information shared included threats, vulnerabilities, suspicious activities, and Coast Guard strategies to protect port infrastructure. The AMSCs also served as a forum for developing Area Maritime Security Plans. While establishing AMSCs has increased information sharing among port stakeholders, our earlier work noted that the lack of federal security clearances for non-federal members of committees hindered some information sharing. To address this issue, we made recommendations to ensure that non-federal officials received needed security clearances in a timely manner. The Coast Guard agreed with our recommendations and has since taken actions to address them, including (1) distributing memos to field office officials clarifying their role in granting security clearances to AMSC members, (2) developing a database to track the recipients of security clearances, and (3) distributing an informational brochure outlining the security clearance process.

Relevant GAO Products

Maritime Security: The SAFE Port Act: Status and Implementation One Year Later. GAO-08-126T. Washington, D.C.: October 30, 2007. See pages 8-11.

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

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

Interagency Operations Centers

Interagency Operations Centers

Interagency Operations Centers (IOCs) are physical or virtual centers of collaboration to improve maritime domain awareness and operational coordination among port partners—including federal, state, and local law enforcement agencies. These port partners use these centers to participate in maritime security activities, such as the implementation and administration of intelligence activities, information sharing, and vessel tracking.

The SAFE Port Act required the establishment of certain IOCs, and the Coast Guard Authorization Act of 2010 further specified that IOCs should provide, where practicable, for the physical collocation of the Coast Guard with its port partners, where practicable, and that IOCs should include information-management systems (46 U.S.C. § 70107A).

To facilitate IOC implementation and the sharing of information across IOC participants, the Coast Guard began implementing a web-based information management and sharing system called WatchKeeper in 2005.

Appropriations Information

The Coast Guard received \$60 million in appropriations in fiscal year 2008 that Congress directed the Coast Guard to use to begin the process of establishing IOCs. The Coast Guard received an additional \$14 million in congressionally-directed appropriations from fiscal years 2009 through 2012 to fund IOC implementation, for a total of \$74 million in IOC funding since fiscal year 2008.

Summary of Key Findings and Recommendations

Our work on IOCs found that they provided promise in improving maritime domain awareness and information sharing. The Departments of Homeland Security, Defense, and Justice all participated to some extent in three early prototype IOCs. These IOCs improved information sharing through the collection of real time operational information. Thus, IOCs can provide continuous information about maritime activities and directly involve participating agencies in operational decisions using this information. For example, agencies have collaborated in vessel boardings, cargo examinations, and enforcement of port security zones. In February 2012, however, we reported that the Coast Guard did not meet the SAFE Port Act's deadline to establish IOCs at all high-risk ports within 3 years of enactment. This was due, in part because the Coast Guard was not appropriated funds to establish the IOCs in a timely manner and because the definition of a fully operational IOC was evolving during this period. As of October 2010—the most recent date for which we had data available—32 of the Coast Guard's 35 sectors had made progress in implementing IOCs, but none of the IOCs had achieved full operating capability. In our February 2012 report, we made several recommendations to the Coast Guard to help ensure effective implementation and management of its WatchKeeper information sharing system, such as revising the integrated master schedule. DHS concurred with the recommendations, subject to the availability of funds.

Relevant GAO Products

Maritime Security: Coast Guard Needs to Improve Use and Management of Interagency Operations Centers. GAO-12-202. Washington, D.C.: February 13, 2012.

Maritime Security: The SAFE Port Act: Status and Implementation One Year Later. GAO-08-126T. Washington, D.C.: October 30, 2007. See pages 8-11.

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

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

Vessel Tracking

Vessel Tracking

Vessel tracking activities are those used to track vessels at sea and in coastal areas in order to attempt to determine the degree of risk presented by each vessel while minimizing disruption on the marine transportation system. Within DHS, the Coast Guard has programs and uses several technologies to track vessels. In general, these vessel tracking systems work for larger commercial vessels, such as those 300 gross tons or more, with requirements to have the tracking technologies. These systems are not effective at tracking smaller vessels, which can present a threat to larger vessels and maritime infrastructure.

MTSA included the first federal vessel tracking requirements to improve the nation's security by mandating that certain vessels operate an automatic identification system—a tracking system used for identifying and locating vessels—while in U.S. waters (46 U.S.C. § 70114). MTSA also allowed for the development of a long-range automated vessel tracking system that would track vessels at sea based on existing onboard radio equipment and data communication systems that can transmit the vessel's identity and position to rescue forces in the case of an emergency. Later, the Coast Guard and Maritime Transportation Act of 2004 amended MTSA to require the development of a long-range tracking system (46 U.S.C. § 70115).

Funding Information

Funding for vessel tracking is not specifically identified in the DHS budget and so we were not able to determine costs allocated for the program. In March 2009, however, we reported that the Coast Guard expected its long-range identification and tracking system, one element of vessel tracking, to cost \$5.3 million in fiscal year 2009 and approximately \$4.2 million per year after that. We also noted in that report that long-range automatic identification system technology, another vessel tracking effort, was not far enough along to know how much it would cost.

Summary of Key Findings and Recommendations

Our work on vessel tracking found that the Coast Guard has developed a variety of vessel tracking systems that provide information key to identifying high risk vessels and developing a system of security measures to reduce risks associated with them. We reported on the Coast Guard's early efforts to develop a vessel information system, as well as more recent efforts to develop an automatic information system to track vessels at sea. Our work in the vessel tracking area showed opportunities for the Coast Guard to reduce costs and eliminate duplication. For example, in July 2004 we reported that some local port entities were willing to assume the expense and responsibility for automatic information tracking if they were able to use the data, along with the Coast Guard, for their own purposes. Further, in March 2009, we reported that the Coast Guard was using three different means to track large vessels at sea, resulting in potential duplication in information provided. As a result, we made several recommendations to reduce costs, including that the Coast Guard partner with local ports and analyze the extent to which duplicate information is needed to track large vessels. In general, the Coast Guard concurred with our recommendations and has taken steps to partner with local port entities and analyze the performance of vessel tracking systems.

Relevant GAO Products

Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed. GAO-09-337. Washington, D.C.: March 17, 2009.

Maritime Security: Partnering Could Reduce Federal Costs and Facilitate Implementation of Automatic Vessel Identification System. GAO-04-868. Washington, D.C.: July 23, 2004.

Coast Guard: Vessel Identification System Development Needs to Be Reassessed. GAO-02-477. Washington, D.C.: May 24, 2002.

Automated Targeting System

Automated Targeting System

The Automated Targeting System (ATS) is a computerized model that CBP officers use as a decision support tool to help them identify and target maritime cargo containers for inspection. ATS was developed in the aftermath of the terrorist attacks of September 11, 2001 to address the concern that terrorists might attempt to smuggle a weapon of mass destruction into the United States using one of the millions of cargo containers that arrive at our nation's seaports. CBP uses ATS as part of its mission to enhance container security and reduce the vulnerabilities associated with the supply chain—the flow of goods from manufacturers to retailers. Specifically, CBP uses ATS to identify high-risk containers that require additional research or inspection at foreign or U.S. seaports.

In 2006, the SAFE Port Act required that DHS collect additional data to identify high-risk cargo for inspection (6 U.S.C. § 943(b)). In response to this requirement, in January 2009, CBP implemented the Importer Security Filing and Additional Carrier Requirements, collectively known as the 10+2 rule. Under this rule, importers are required to provide CBP with additional information, such as customs entry information, and carriers are required to provide CBP with information, such as cargo manifest and vessel stowage information. The collection of this additional cargo information is intended to further enhance CBP's ability to use ATS to identify high-risk shipments.

Table 4: Total ATS Obligations, Fiscal Year 2005 through May 2012 (in millions)

ATS	Fiscal year							
	2005	2006	2007	2008	2009	2010	2011	2012*
Obligations	29.8	27.9	26.8	26.8	32.5	32.6	32.4	7.7
Total for all years	\$216.5							

Source: DHS.

*Represents fiscal year obligations through May 2012.

Summary of Key Findings and Recommendations

Our work on ATS has shown that CBP made progress in implementing ATS and enhancing it through the use of additional data. For example, in March 2004, we reported that CBP has (1) refined ATS to target high risk cargo containers for physical inspection, (2) implemented national targeting training, and (3) sought to improve the quality and timeliness of manifest information. Also, in response to our 2004 recommendation that CBP initiate an external peer review of ATS, CBP contracted with a consulting firm to evaluate CBP's targeting methodology and recommend improvements. Our September 2010 report regarding the additional information required by the 10+2 rule indicated that the new information on vessel stow plans enabled CBP to identify containers with incomplete manifest data, which are inherently higher risk. We also reported, however, that CBP had not yet incorporated the new information and recommended that it set time frames and milestones for updating its national security targeting criteria. CBP generally concurred with our recommendations and has begun to address them. We are in the process of completing an updated review of ATS for the House Committee on Energy and Commerce and anticipate issuing a report later this year.

Relevant GAO Products

Supply Chain Security: CBP Has Made Progress in Assisting the Trade Industry in Implementing the New Importer Security Filing Requirements, but Some Challenges Remain. GAO-10-841. Washington, D.C.: September 10, 2010.

The SAFE Port Act: Status and Implementation One Year Later. GAO-08-126T. Washington, D.C.: October 30, 2007. See pages 6 and 27-28.

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.

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

Advanced Spectrographic Portal Program

Advanced Spectrographic Portal Program

The advanced spectroscopic portal (ASP) program was designed to develop and deploy a more advanced radiation portal monitor to detect and identify radioactivity coming from containers and trucks at seaports and land border crossings. From 2005 to 2011, DNDO was developing and testing the ASP and planned to use these machines to replace some of the currently deployed radiation portal monitors used by CBP at ports-of-entry for primary screening, as well as the handheld identification devices currently used by CBP for secondary screening. If they performed well, DNDO expected that the ASP could (1) better detect key threat material and (2) increase the flow of commerce by reducing the number of referrals for secondary inspections. However, ASPs cost significantly more than currently deployed portal monitors. We estimated in September 2008 that the lifecycle cost of each ASP (including deployment costs) was about \$822,000, compared with about \$308,000 for radiation portal monitors, and that the total program cost for DNDO's latest plan for deploying radiation portal monitors—including ASPs—would be about \$2 billion.

Funding Information

Overall, DHS spent more than \$280 million developing and testing the ASP program.

Summary of Key Findings and Recommendations

In September 2007, we found that DNDO's initial testing of the ASP were not an objective and rigorous assessment of the ASP's capabilities. For example, DNDO used biased test methods that enhanced the performance of the ASP during testing. At the same time, DNDO did not use a critical CBP standard operating procedure for testing deployed equipment. We made several recommendations about improving the testing of ASPs which DNDO subsequently implemented. In May 2009, we reported that DNDO improved the rigor of its testing; however, this improved testing revealed that the ASPs had a limited ability to detect certain nuclear materials at anything more than light shielding levels. In particular, we reported that ASPs performed better than currently deployed radiation portal monitors in detecting nuclear materials concealed by light shielding, but differences in sensitivity were less notable when shielding was slightly below or above that level. In addition, further testing in CBP ports revealed too many false alarms for the detection of certain high-risk nuclear materials. According to CBP officials, these false alarms are very disruptive in a port environment in that any alarm for this type of nuclear material would cause CBP to take enhanced security precautions because such materials (1) could be used in producing an improvised nuclear device and (2) are rarely part of legitimate or routine cargo. In 2012, we reported that once ASP testing became more rigorous, these machines did not perform well enough to warrant deployment. Accordingly, DHS scaled back the program in 2010 and later cancelled the program in July 2012.

Relevant GAO Products

Combating Nuclear Smuggling: DHS has Developed Plans for Its Global Nuclear Detection Architecture, but Challenges Remain in Deploying Equipment. GAO-12-941T. Washington D.C.: July 26, 2012.

Combating Nuclear Smuggling: DHS Improved Testing of Advanced Radiation Detection Portal Monitors, but Preliminary Results Show Limits of the New Technology. GAO-09-655. Washington D.C.: May 21, 2009.

Combating Nuclear Smuggling: DHS's Program to Procure and Deploy Advanced Radiation Detection Portal Monitors Is Likely to Exceed the Department's Previous Cost Estimates. GAO-08-1108R. Washington, D.C.: September 22, 2008.

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

Container Security Initiative

Container Security Initiative

The Container Security Initiative (CSI) is a bilateral government partnership program to station CBP officers at foreign seaports where they identify U.S.-bound shipments at risk of containing weapons of mass destruction or other terrorist contraband. CBP launched CSI in January 2002 in an effort to protect global trade lanes by targeting and examining high-risk containers as early as possible in their movement through the global supply chain. The program was meant to address concerns (after the terrorist attacks of September 11, 2001), that terrorists could smuggle weapons of mass destruction inside containers bound for the United States.

As part of the program, foreign governments allow CBP officers in the CSI program to work closely with host customs officials. CBP officers at the CSI seaports are responsible for targeting U.S.-bound high-risk cargo shipped in containers and other tasks, whereas host government customs officials examine the high-risk cargo—when requested by CBP—by scanning containers using various types of nonintrusive inspection equipment or by physically searching the containers before they are loaded onto vessels bound for the United States. By fiscal year 2007 CBP reached its goal of operating CSI in 58 foreign seaports, which collectively accounted for more than 80 percent of the cargo shipped to the United States.

Table 5: Total CSI and Secure Freight Initiative (SFI) Obligations, Fiscal Year 2004 through May 2012 (in millions)

CSI and SFI*	Fiscal year								
	2004	2005	2006	2007	2008	2009	2010	2011	2012 ^b
Obligations	61.4	126.1	138.0	138.5	145.9	148.9	145.5	106.9	51.6
Total for all years									\$1,062.8

Source: DHS.

*We were unable to distinguish between CSI and SFI obligations because they are funded out of the same budget line item.

^bRepresents fiscal year obligations through May 2012.

Summary of Key Findings and Recommendations

Our work on CSI showed that the program has matured and improved, meeting its strategic goals by increasing both the number of CSI locations and the proportion of total U.S.-bound containers passing through CSI ports. In addition, relationships with host governments have improved over time, leading to increased information sharing between governments and a bolstering of host government customs and port security practices. Our reports made recommendations to CBP to further strengthen the CSI program by, among other things, revising its staffing model, developing performance measures, and improving its methods for conducting on-site evaluations. CBP generally agreed with our recommendations and has taken actions to address them. For example, in response to one of our recommendations, in January 2009, CBP began transferring CSI staff from overseas ports to perform targeting remotely from the National Targeting Center in the United States. As part of this effort, foreign staffing levels for CSI decreased and CBP was able to decrease the program's operating costs by over \$35 million.

Relevant GAO Products

Supply Chain Security: Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning. GAO-12-422T. Washington, D.C.: February 7, 2012. See pages 12-13.

Supply Chain Security: Examinations of High-Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed. GAO-08-187. Washington, D.C.: January 25, 2008.

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.

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

Megaports Initiative

Megaports Initiative

The Megaports Initiative seeks to deter, detect, and interdict nuclear or other radiological materials smuggled through foreign seaports. Established by the Department of Energy (DOE) in 2003, the Initiative funds the installation of radiation detection equipment at select seaports overseas. The Initiative trains foreign personnel to use this equipment to scan shipping containers entering and leaving these seaports—regardless of destination—for nuclear and other radioactive material that could be used against the United States or its allies.

To help decision-makers identify and prioritize foreign seaports for participation in the Megaports Initiative, DOE uses a model that ranks foreign ports according to their relative attractiveness to potential nuclear smugglers. The Maritime Prioritization Model incorporates information, such as port security conditions, volume of container traffic passing through ports, the proximity of the ports to sources of nuclear material, and the proximity of the ports to the United States. The model is updated regularly to incorporate new information.

Table 6: Total Megaports Expenditures, Fiscal Year 2003 through December 2011 (in millions)

Megaports Initiative	Fiscal year									
	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Expenditure amount ^a	1.3	56.4	60.9	57.1	88.7	102.7	136.4	167.3	145.1	33.8
Total for all years	\$849.8									

Source: DOE

^aExpenditures are expressed in constant dollars. The total for fiscal year 2012 is as of December 2011.

Summary of Key Findings and Recommendations

We reported in March 2005 that the Megaports Initiative had established Megaports at two seaports—Rotterdam, the Netherlands, which is the largest port in Europe, and Piraeus, Greece, where security concerns had increased prior to the 2004 Olympic Games. DOE had trained foreign customs officials and provided radiation detection equipment to both seaports. However, we also reported that the Initiative had limited success in initiating work at seaports identified as high priority. Among other things, we reported that it was difficult to gain the cooperation of foreign governments, in part because some countries were concerned that scanning large volumes of containers would create delays, thereby inhibiting the flow of commerce at their ports. We also found that the Initiative did not have a comprehensive long-term plan to guide the Initiative's efforts and faced several operational and technical challenges in installing radiation detection equipment at foreign seaports. We also previously reported that DOE had faced several operational and technical challenges specific to installing and maintaining radiation detection equipment, including ensuring the ability to detect radioactive material, overcoming the physical layout of ports and cargo container-stacking configurations, and sustaining equipment in port environments with high winds and sea spray. We recommended that DOE (1) develop a comprehensive long-term plan for the Initiative that identifies criteria for deciding how to strategically set priorities for establishing Megaports and (2) reevaluate cost estimates and adjust long-term projections as necessary. DOE has implemented both recommendations. We are currently updating our work on the Megaports Initiative and expect to issue a report later this year.

Relevant GAO Products

Maritime Security: The SAFE Port Act: Status and Implementation One Year Later. GAO-08-126T. Washington, D.C.: October 30, 2007. See pages 41-42.

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 31, 2005.

Secure Freight Initiative

Secure Freight Initiative

The Secure Freight Initiative (SFI) established pilot projects to test the feasibility of scanning 100 percent of U.S.-bound containers at foreign ports to address concerns that terrorists would smuggle weapons of mass destruction (WMD) inside cargo containers bound for the United States. CBP shares responsibility for the initiative with the State Department and the Department of Energy (DOE) as part of its responsibilities for overseeing oceangoing container security and reducing the vulnerabilities associated with the supply chain.

SFI was created, in part, due to statutory requirements. The SAFE Port Act requires that pilot projects be established at three ports to test the feasibility of scanning 100 percent of U.S.-bound containers at foreign ports (6 U.S.C. § 981). In August 2007, 2 months before the pilot began operations, the implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) was enacted, which requires, among other things, that by July 2012, 100 percent of all U.S.-bound cargo containers be scanned before being placed on a vessel at a foreign port, with possible extensions for ports under certain conditions (6 U.S.C. § 982(b)). Ultimately, CBP implemented SFI at six ports.

Logistical, technological, and other challenges prevented the participating ports from achieving 100 percent scanning and DHS and CBP have since reduced the scope of the SFI program from six ports to one. Further, in May 2012, the Secretary of Homeland Security issued a 2-year extension for all ports, thus delaying the implementation date for 100 percent scanning until July 2014.

Obligations Information

Obligations for this initiative are included with obligations for the Container Security Initiative, as shown in table 5 above.

Summary of Key Findings and Recommendations

We reported in October 2009 that CBP and DOE have been successful in integrating images and radiological signatures of scanned containers onto a computer screen that can be reviewed remotely from the United States. They have also been able to use SFI as a test bed for new applications of existing technology, such as mobile radiation scanners. However, we reported in June 2008 that CBP has faced difficulties in implementing SFI due to challenges in host nation examination practices, performance measures, resource constraints, logistics, and technology limitations. We recommended in October 2009 that DHS, in consultation with the Secretaries of Energy and State, conduct cost-benefit and feasibility analyses and provide the results to Congress. CBP stated it does not plan to develop comprehensive cost estimates because SFI has been reduced to one port and it has no funds to develop such cost estimates. DHS and CBP have not performed a feasibility assessment of 100 percent scanning to inform Congress as to what cargo scanning they can do, so this recommendation has not yet been addressed. We will continue to monitor DHS and CBP actions that could address this recommendation.

Relevant GAO Products

Supply Chain Security: Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning. GAO-12-422T. Washington, D.C.: February 7, 2012. See pages 15-19.

Maritime Security: Responses to Questions for the Record. GAO-11-140R. Washington, D.C.: October 22, 2010. See pages 17-21.

Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers. GAO-10-12. Washington, D.C.: October 30, 2009.

CBP Works with International Entities to Promote Global Customs Security Standards and Initiatives, but Challenges Remain. GAO-08-538. Washington, D.C.: August 15, 2008. See pages 31-34.

Supply Chain Security: Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers. GAO-08-533T. Washington, D.C.: June 12, 2008.

Customs-Trade Partnership Against Terrorism

Customs-Trade Partnership Against Terrorism

The Customs-Trade Partnership Against Terrorism (C-TPAT) program is a voluntary program that enables CBP officials to work in partnership with private companies to review and approve the security of their international supply chains. In November 2001, CBP announced the C-TPAT program as part of its efforts toward facilitating the free flow of goods while ensuring that the containers do not pose a threat to homeland security. In October 2006, the SAFE Port Act established a statutory framework for the C-TPAT program, codified its existing membership processes, and added new components—such as time frames for certifying, validating, and revalidating members' security practices (6 U.S.C. §§ 961-973).

Companies that join the C-TPAT program commit to improving the security of their supply chains and agree to provide CBP with information on their specific security measures. In addition, the companies agree to allow CBP to verify, among other things, that their security measures meet or exceed CBP's minimum security requirements. This allows CBP to ensure that the security measures outlined in a member's security profile are in place and effective. In return for their participation in the program, C-TPAT members are entitled a reduced likelihood of scrutiny of their cargo. CBP has awarded initial C-TPAT certification—or acceptance of the company's agreement to voluntarily participate in the program—to over 10,000 companies, as of February 2012.

Table 7: Total C-TPAT Obligations, Fiscal Year 2005 through May 2012 (in millions)

C-TPAT	Fiscal year									
	2004	2005	2006	2007	2008	2009	2010	2011	2012 ^a	
Obligations	14.0	37.8	67.4	49.7	57.4	52.4	46.5	44.5	23.6	
Total for all years										\$393.5

Source: DHS.

^aRepresents fiscal year obligations through May 2012.

Summary of Key Findings and Recommendations

We reported in April 2008 that the program holds promise as part of CBP's multifaceted maritime security strategy. The program allows CBP to develop partnerships with the trade community, which is a challenge given the international nature of the industry and resulting limits on CBP's jurisdiction and activities. C-TPAT provides CBP with a level of information sharing that would otherwise not be available. However, our reports raised a number of concerns about the overall management of the program and its challenges in verifying that C-TPAT members meet security criteria. We recommended that CBP strengthen program management by developing planning documents, performance measures, and improving the process for validating security practices of C-TPAT members. CBP agreed with these recommendations and has addressed them.

Relevant GAO Products

Supply Chain Security: Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning. GAO-12-422T. Washington, D.C.: February 7, 2012. See pages 13-14.

Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers. GAO-10-12. Washington, D.C.: October 30, 2009. See pages 41-43.

Supply Chain Security: U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices. GAO-08-240. Washington, D.C.: April 25, 2008.

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

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

Mutual Recognition Arrangements

Mutual Recognition Arrangements

Mutual recognition arrangements (MRAs) allow for the supply chain security-related practices and programs taken by the customs administration of one country to be recognized by the administration of another. As of July 2012, CBP has made such arrangements with five countries and an economic union as part of its efforts to partner with international organizations and develop supply chain security standards that can be implemented throughout the international community.

According to CBP, a network of mutual recognition could lead to greater efficiency in improving international supply chain security by, for example, reducing redundant examinations of cargo containers and avoiding the unnecessary burden of addressing different sets of requirements as a shipment moves throughout the global supply chain. CBP and other international customs officials see mutual recognition arrangements as providing a possible strategy for the CSI program (which includes stationing CBP officers abroad). As of July 2012, CBP had signed six mutual recognition arrangements.

Budget Authority Information

MRA are included in the Other International Programs budget line item, but there is no specific line item for these activities. As such, we were unable to determine MRA obligations information.

Summary of Key Findings and Recommendations

In our work on international supply chain security we reported that CBP has recognized that the United States is no longer self-contained in security matters—either in its problems or its solutions. That is, the growing interdependence of nations necessitates that policymakers work in partnerships across national boundaries to improve supply chain security. We also reported that other countries are interested in developing customs-to-business partnership programs similar to CBP's C-TPAT program. Other countries are also interested in bi-lateral or multi-lateral arrangements with other countries to mutually recognize each others' supply chain container security programs. For example, officials within the European Union and elsewhere see the C-TPAT program as one potential model for enhancing global supply chain security. Thus, CBP has committed to promoting mutual recognition arrangements based on an international framework of standards governing customs and related business relationships in order to enhance global supply chain security. Our work on other programs indicated that CBP does not always have critical information on other countries' customs examination procedures and practices, even at CSI ports where we have stationed officers. However, our reports to date have not made any specific recommendations related to mutual recognition arrangements.

Relevant GAO Products

Supply Chain Security: Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning. GAO-12-422T. Washington, D.C.: February 7, 2012. See pages 13-14.

Supply Chain Security: CBP Works with International Entities to Promote Global Customs Security Standards and Initiatives, but Challenges Remain. GAO-08-538. Washington, D.C.: August 15, 2008. See pages 23-31.

Supply Chain Security: Examinations of High-Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed. GAO-08-187. Washington, D.C.: January 25, 2008. See pages 33-40.

International Port Security Program

International Port Security Program

The International Port Security Program (IPSP) provides for the Coast Guard and other countries' counterpart agencies to visit and assess the implementation of security measures in each others' ports against established security standards. The underlying assumption for the program is that the security of domestic ports also depends upon security at foreign ports where vessels and cargoes bound for the United States originate.

MTSA required the Coast Guard to develop such a program to assess security measures in foreign ports and, among other things, recommend steps necessary to improve security measures in those ports. To address this requirement, the Coast Guard established the International Port Security Program in April 2004. Subsequently, in October 2006, the SAFE Port Act required the Coast Guard to reassess security measures at such foreign ports at least once every 3 years (46 U.S.C. §§ 70108, 70109).

In implementing the program, the Coast Guard uses the International Maritime Organization's International Ship and Port Facility Security (ISPS) Code. This code serves as the benchmark by which it measures the effectiveness of a country's antiterrorism measures in a port. Coast Guard teams conduct country visits, discuss implemented security measures, and collect and share best practices to help ensure a comprehensive and consistent approach to maritime security in ports worldwide.

Budget Authority Information

Activities related to the International Port Security Program are not specifically identified in the Coast Guard budget. Such activities fall under the Coast Guard's ports, waterways and coastal security mission. See table 1 for the reported budget authority for that mission for fiscal years 2004 through 2013.

Summary of Key Findings and Recommendations

Our work on the International Port Security Program found that the Coast Guard had made progress in visiting and assessing port security in foreign ports. We reported in October 2007 that the Coast Guard had visited more than 100 countries and found that most of the countries had substantially implemented the ISPS code. The Coast Guard had also consulted with a contractor to develop a more risk-based approach to planning foreign country visits, such as incorporating information on corruption and terrorist activities levels within a country. The Coast Guard has made progress despite a number of challenges. For example, the Coast Guard has been able to alleviate challenges related to sovereignty concerns of some countries by including a reciprocal visit feature in which the Coast Guard hosts foreign delegations to visit U.S. ports and observe ISPS Code implementation in the United States. Another challenge program officials overcame was the lack of resources to improve security in poorer countries. Specifically, Coast Guard officials worked with other federal agencies (e.g., the Departments of Defense and State) and international organizations (e.g., the Organization of American States) to secure funding for training and assistance to poorer countries that need to strengthen port security efforts.

Relevant GAO Products

Maritime Security: DHS Progress and Challenges in Key Areas of Port Security. GAO-10-940T. Washington, D.C.: July 21, 2010. See pages 10-11.

Maritime Security: The SAFE Port Act: Status and Implementation One Year Later. GAO-08-126T. Washington, D.C.: October 30, 2007. See pages 15-19.

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

Appendix II: GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this statement include Christopher Conrad (Assistant Director), Adam Anguiano, Aryn Ehlow, Alyson Goldstein, Paul Hobart, Amanda Kolling, Glen Levis, and Edwin Woodward. Additional contributors include Frances Cook, Tracey King, and Jessica Orr.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."
Order by Phone	<p>The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.</p> <p>Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.</p> <p>Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.</p>
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov .
To Report Fraud, Waste, and Abuse in Federal Programs	<p>Contact:</p> <p>Website: http://www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470</p>
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov , (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov , (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548



Please Print on Recycled Paper.



AMERICAN ASSOCIATION OF PORT AUTHORITIES
1010 Duke Street • Alexandria, VA 22314
Phone: (703) 684-5700 • Fax: (703) 684-6321

Testimony of Bethann Rooney
Manager, Port Security at
The Port Authority of New York and New Jersey
On Behalf of the
American Association of Port Authorities

Before the
The United States House of Representatives
Committee on Transportation & Infrastructure
Subcommittee on Coast Guard and Maritime Transportation

Hearing: *"Tenth Anniversary of the Maritime Transportation Security Act:
Are We Safer?"*

September 11, 2012
10:00 a.m.

Good morning. I am Bethann Rooney, Manager of Port Security at The Port Authority of New York and New Jersey. I am testifying today on behalf of the American Association of Port Authorities (AAPA), where I serve as Chairman of the Port Security Caucus and a member of the AAPA Security Committee. My testimony today is on behalf of the AAPA's 81 U.S. members. AAPA port members are public entities, divisions or agents of state and local governments mandated by law to serve the public by developing, maintaining and operating port facilities.

I had the pleasure of testifying before this Subcommittee on the "Implementation of the Maritime Transportation Security Act of 2002" in June of 2003 and I am pleased to be here again today to discuss the implementation of the Act over the past decade.

Prior to 9/11, security was not a top concern for most U.S. ports. That changed in an instant after that tragic day, and Congress and the Administration took quick and decisive action to help focus on the risk to our seaports. Enhancing maritime security and protecting our ports from acts of terrorism and other crime remains a top priority for the AAPA and U.S. ports authorities.

Protecting America's ports is critical to our nation's economic growth and vitality, and is an integral part of homeland security and national defense. Ports handle 99 percent of our overseas (non-NAFTA) cargo by volume and enable the deployment of our Armed Services. America's consumer-driven market relies upon a very efficient logistics chain, of which our ports are a critical part, to facilitate the just-in-time delivery system. Shippers want their goods moved in the fastest, most reliable, cheapest and most secure method. The challenge for the past ten (10) years has been to integrate security into the efficient and economic flow of commerce.

The MTSA was groundbreaking legislation that authorized the United States Coast Guard and other agencies to establish maritime security standards and mandate security enhancements to ports, terminals and vessels. The cornerstone of these new mandates was a requirement for vessels and facilities to conduct vulnerability assessments and develop Vessel and Facility Security Plans. We commend the U.S. Coast Guard for its excellent job in developing the regulations — both the initial plans in 2004 and the subsequent updated plans in 2009 — for enforcing those regulations and for working in partnership with the industry to secure our ports.

Security Plans and Assessments

Port and vessel security is a continuous activity that requires constant attention on the part of many individuals. Therefore, the process of renewing the Facility Security Plans every five (5) years is relatively simple with minimal to no cost required. The cost of meeting and maintaining the requirements of the security regulations, however, is significant.

Implementing MTSA is not a one-time expense, but rather requires the expenditure of recurring costs in order to operate, maintain and staff the security equipment, systems, and processes put in place. For example, in 2003, the Port Authority of New York & New Jersey estimated that we would spend \$32.5 million to implement the Maritime Transportation Security Act, but during the past eleven (11) years, the Port Authority has invested more than \$166 million on port security.

The foundation of a robust security plan and program is a comprehensive and accurate risk assessment. While tremendous progress has been made throughout the Department of Homeland Security in this area in the past ten (10) years, it is AAPA's belief that there is still room for improvement. In the Coast Guard regulations, guidance is provided on what should be included in a Facility Security Assessment. Both this guidance and the online assessment tool that was made available by the Transportation Security Administration (TSA) to port facilities amount to little more than a physical security survey and a checklist of how the facility meets the regulatory requirements, rather than a detailed risk assessment.

Over the years the Coast Guard's Maritime Security Risk Assessment Model, or MSRAM, which was developed in response to Section 70102 of the MTSA, has evolved into a very robust and comprehensive risk assessment tool. For example, in the Port of New York and New Jersey, more than 3,200 threat scenarios have been evaluated for nearly 400 pieces of Maritime Critical Infrastructure/Key Resources (MCI/KR). It is a dynamic tool that is used regularly to inform our force protection plans, resource allocations, grant award decisions and strategic risk management decisions. To be most effective, AAPA believes that MSRAM should be used uniformly by all federal agencies that assess risk in the maritime environment. Additionally, MSRAM should be made available in an unclassified version, on a limited basis to regulated facilities and vessels to conduct detailed risk assessments of their own facilities or vessels using the same scoring criteria that the Coast Guard uses. This provision is included in the Coast Guard Authorization Act of 2010 by the 111th Congress, but has not been implemented yet.

Port Security Grant Program

Key to enhancing and maintaining the security of ports is the Port Security Grant Program. It provides much needed help to port facilities to harden security to protect these vital ports of entry from acts of terrorism. Since its inception, the program has provided more than \$2.7 billion in grants to harden security at port facilities.

Through fiscal year 2009, Congress has appropriated the authorized level of \$400 million annually for the Port Security Grant program. However, in the past few years, Congressional support for all Homeland Security Grants, including the Port Security Grant Program has eroded. In fiscal year 2012, Congress appropriated \$1.3 billion for all Homeland Security Grants

(a 40 percent cut over the previous year) and gave the DHS Secretary the authority to determine the final funding level for each individual program. Only \$97.5 million was allocated in fiscal year 2012 for port security. Our economy, our safety and our national defense depend largely on how well we can protect our seaports, and cuts in federal funding present significant challenges in the security of our ports. According to the 9/11 Commission Report, "opportunities to do harm are as great, or greater, in maritime and surface transportation" as they are in aviation. We urge Congress to provide full funding for the Port Security Grant Program so that our ports continue to be a priority in our country's war against terrorism.

DHS is also proposing a move to merge all grant programs into one single program that would fund all critical infrastructure segments (i.e., Transit, Inter-City Rail, Urban Area Security Initiative and Emergency Management Performance Grants). The States would manage this new program, a move that the AAPA strongly opposes. We encourage your Committee to continue to voice opposition to this new structure.

From FY07 through FY11, all Group 1 and 2 ports were designated a sum of money based on a national risk analysis. The decision on grant awards to individual applicants in each port area was left to a group of local experts who were appointed by the Coast Guard Captain of the Port. Then in FY12, all ports competed for a share of funding in their corresponding group and decisions on award allocations were made by DHS. The result is that DHS gave small amounts of funding to many projects rather than fully funding the higher priority projects that in the opinion of local experts mitigated higher risks. If the grants remain competitive, AAPA believes that more weight should be given to recommendations of the local experts so that risks are not created when projects are not fully funded or cannot be completed without sufficient funding.

In these tight economic times, 25 percent cost-share for public agencies is a disincentive to making additional security enhancements, updating or replacing outdated security systems and equipment installed up to ten years ago, and implementing the outstanding initiatives in the DHS-approved Port-Wide Strategic Risk Management Plans for each port area. The Port Security Grant Program is one of a few DHS grant programs that requires a cost-share. Transit grants, urban area security initiative and state homeland security grants, for example, are all exempt from cost-share requirements. At a minimum, AAPA urges Congress to direct the Department to eliminate the cost-share requirement for public agencies and their tenants.

A major challenge with the Port Security Grant Program, one that has received ongoing attention from both Congress and the Administration, is the rate at which funds are spent or that the monies which have been awarded are drawn down. As of July 2012, FEMA reports that more than \$1.6 billion has been awarded since FY07. Approximately \$220 million or 15 percent, however, remains on hold pending federal reviews or the identification of suitable projects. Of the funding that is currently available to be spent, approximately one third has been drawn down already. It is important to understand, however, that the remaining two thirds of the funding is not sitting idle. Work is being done and projects are underway to spend the funding in accordance with the federal rules and guidelines that govern these grants.

The fact remains that for a number of reasons grant spending is not as quick as we would all like it to be. For starters, AAPA members have found that there is a significant time delay between when DHS announces the awards and when FEMA finally completes all of the reviews (budget and environmental and historic reviews) and gives grantees approval to begin making these security improvements. While significant improvements have been made in this area, AAPA believes that further streamlining is still possible to help get the funding out more quickly.

Grantees then need to follow their own internal procurement policies, which for public agencies like our member port authorities can take six to nine months just for a public RFP process to be completed before the contracts are even awarded. Once a project gets underway, there is a lag between when the funds are spent and reimbursement is sought from the federal government, which our members are working to address. The move, however, to shorten the performance period from three years to two years is not going to expedite spending but rather add additional burden to grantees who will need to justify and request an extension simply because the process generally doesn't allow spending to occur quicker. We ask for this Committee's assistance to ensure that the performance period for Port Security Grant funding is no less than three years. Furthermore, it is imperative that extension requests be reviewed expeditiously and be considered for a minimum of one-year increments.

We commend Secretary Napolitano and FEMA for their announcement earlier this year on a series of measures that provide grantees with additional flexibility to accelerate the spending of their remaining FY07 – FY11 grant funds. These measures enable grantees to apply grant balances to more urgent priorities. It also allowed grantees to use funding to cover additional

personnel costs and maintain previously purchased equipment which was all originally authorized under the Maritime Transportation Security Act but not fully implemented.

Radiation Portal Monitors

The MTSA also authorized grant funding to be used for "the cost of screening equipment, including equipment that detects weapons of mass destruction and conventional explosives, and the testing and evaluating of such equipment to certify secure systems of transportation."

Unfortunately, in accordance with grant guidance and Office of Management and Budget requirements, grant funding cannot be used for purchases or services that support a federal function. Cargo inspection or the process of ensuring that goods entering the United States are free from the presence of restricted or prohibited items like weapons of mass destruction and explosives is a federal function.

When the DHS budget fully funded this function, particularly the installation and maintenance of the Radiation Portal Monitors (RPMs) that Customs and Border Protection (CBP) uses to scan 100 percent of import containers that enter our ports, the limitations on the use of grant funding for screening equipment was not a problem. Today, the Domestic Nuclear Detection Office (DNDO) and CBP are fiscally constrained and are asking port authorities and marine terminal operators to share the cost of the installation and maintenance of DHS-owned, -operated and -controlled equipment. This includes all of the engineering, permits and installation costs, infrastructure such as fiber, electrical, plumbing, foundations and protective barriers as well as the associated office space for CBP personnel including furniture, telephone and data lines. To give you an example, for one project in the Port of New York and New Jersey, it is estimated that our terminal operator will be responsible for nearly \$2.5 million while DHS will contribute approximately \$750,000 for the same project.

As imports increase, container terminals must reconfigure, expand or be newly developed to keep pace with the growth in global commerce. Each of these facilities requires sufficient detection equipment so that the flow of legitimate commerce is not inhibited. We would like to work with DHS to develop a plan to upgrade obsolete equipment in our ports. Port facilities should not be responsible for paying for DHS equipment. If we are, we should be able to use grant funding to help offset the cost.

Transportation Worker Identification Credential

The last major element of the MTSA that we would like to address is the Transportation Worker Identification Credential (TWIC) program. AAPA and its members have worked closely with TSA and Coast Guard on implementation of the TWIC requirements. We strongly support the TWIC program and look forward to the day when it will be fully implemented.

While the TWIC includes a biometric security feature, it is currently not being used at most facilities due to the lack of a final reader specification and certification process as well as a final rulemaking for the use of the readers. Therefore, the high-tech and high-cost security features imbedded in the TWIC are not being utilized. The visual inspection of TWICs is onerous and prone to errors and complacency. Without readers it is also impossible to identify TWICs that have been reported as being lost, stolen or otherwise revoked or suspended by DHS.

By the end of this year and the first half of 2013, the majority of TWICs will expire. We are pleased that TSA has taken steps to address this issue and are offering an option of paying \$60 to acquire a three-year Extended Expiration Date (EED) card instead of the standard five-year TWIC. However, our member ports are concerned that the lack of an updated threat assessment could compromise the security of our facilities. We are also concerned that the renewal or extension process be convenient and efficient. TSA and their new contractor should again work closely with stakeholders in the maritime environment to educate the workforce regarding these renewal deadlines and requirements, including such issues as enrollment center locations, bulk payments and the availability of on-site enrollments and activations.

When the reader rule is finally published, it is imperative that sufficient time be given to ports to implement the requirements and that adequate port security grant funding be available. TWIC projects should be a top priority of the grant program once the reader rule is released. TWIC projects that were previously awarded funding but could not be completed due to the lack of a reader rule should be funded first. We encourage the Coast Guard to continue their proposed rulemaking process and for TSA to complete the reader evaluation and testing and publication of a Qualified Technology List (QTL).

Enhancements to MTSA

As this Committee considers future enhancements to the MTSA, AAPA respectfully requests you to also consider the following:

- Mutual recognition of U.S. Coast Guard-approved Facility and Vessel Security Plans by CBP for Tier 2 status in the Customs Trade Partnership Against Terrorism (C-TPAT) program.
- Providing marine terminals the equivalent of a "No Fly List" so that we know if TSA has denied a TWIC so that we don't unknowingly allow those individuals access to our facilities with an escort.
- A requirement to display the TWIC on the outermost garment above the waist, similar to what is already required of Security Identification Display Area (SIDA) badge holders in the aviation industry.
- Minimum security standards for maritime support services, including supply vessels, bunker providers and launch operators.
- Identification by vessels of a Security Individual (SI), similar to the Qualified Individual (QI) that they are required to nominate under the Oil Pollution Act of 1990.

Thank you for inviting the Port Authority of New York and New Jersey to testify on the Tenth Anniversary of the Maritime Transportation Security Act. We are safer than we were ten (10) years ago and our agency remains committed to doing its part to protect America.

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

###



WORLD SHIPPING COUNCIL
PARTNERS IN AMERICA'S TRADE

Statement of

Christopher Koch

President & CEO

World Shipping Council

Before the

**House Committee on Transportation & Infrastructure
Subcommittee on Coast Guard and Maritime Transportation**

on

***“Tenth Anniversary of the Maritime Transportation Security Act:
Are We Safer?”***

September 11, 2012

Mr. Chairman and members of the Subcommittee, thank you for the invitation to testify before the Subcommittee today. My name is Christopher Koch. I am President and CEO of the World Shipping Council.¹ WSC members comprise the international liner shipping industry, which transports more than half of the \$1.2 trillion in U.S. ocean-borne commerce. It is clear

¹ The World Shipping Council (WSC) is a non-profit trade association whose goal is to provide a coordinated voice for the liner shipping industry in its work with policymakers and other industry groups with an interest in international transportation. Liner shipping is the sector of the maritime shipping industry that offers regular service based on fixed schedules and itineraries. WSC members carry over 90% of the United States' containerized ocean commerce, and include the full spectrum of carriers from large global lines to niche carriers, offering container, roll on-roll off, and car carrier service as well as a broad array of logistics services. The industry generates over one million American jobs and over \$38 billion of wages annually to American workers. A complete list of WSC members and more information about the Council can be found at www.worldshipping.org.

why the international liner shipping industry has been determined by the Department of Homeland Security (DHS) to be one of the elements of the nation's "critical infrastructure".²

We thank the Committee for the opportunity to participate in today's hearing on the tenth anniversary of the Maritime Transportation Security Act (MTSA) and the efforts that have been taken to increase maritime security.

Maritime Security

For the past decade, the WSC and its member companies have strongly supported the various efforts of the U.S. Coast Guard and U.S. Customs and Border Protection (CBP) to enhance maritime and cargo security. The multi-faceted, risk-based strategies and programs of the government have been able to make substantial progress toward meeting this challenge, and they continue to evolve.

The Coast Guard and CBP recognize the fact that the industry is transporting on average roughly 50,000 containers, holding roughly \$1.8 billion worth of cargo owned by U.S. importers and exporters, each day through U.S. ports. Significant delays to this flow of legitimate commerce could have substantial adverse effects on the American economy. They therefore are attentive to enhancing security, while ensuring and facilitating efficient commerce.

The basic architecture of U.S. maritime security is well known and understandable. First, there is *vessel and port security*, overseen by the Coast Guard and guided in large measure by MTSA and the International Ship and Port Facility Security (ISPS) Code. Second, there is *personnel security*, overseen by various DHS agencies and the State Department. Third, is *cargo*

² The liner industry that has invested over \$400 billion in the vessels, equipment, and marine terminals that are in worldwide operation today. Approximately 1,400 ocean-going liner vessels, mostly containerships, made more than 25,000 calls at ports in the United States during 2010 -- almost 70 vessel calls a day. This industry provides American importers and exporters with door-to-door delivery service for almost any commodity to and from roughly 170 countries. In 2011, approximately 30 million TEU of containerized cargo were imported into or exported from the U.S. In addition to containerships, liner shipping offers services operated by roll-on/roll-off or "Ro-Ro" vessels that are especially designed to handle a wide variety of vehicles, including everything from passenger cars to construction equipment. In 2011, these Ro-Ro ships brought passenger vehicles and light trucks valued at \$72.4 billion into the U.S. and transported units worth \$32.5 billion to U.S. trading partners in other countries. As significant as international liner shipping is, we recognize that it is only one piece of the maritime transportation system that this Subcommittee is reviewing. When one measures trade by cargo weight, 16% of the nation's waterborne imports are delivered by containership. The remaining 84% is delivered via tanker, bulk and break-bulk ships.

security, which for containerized cargo, is addressed through CBP's advance cargo screening program, C-TPAT, and the Container Security Initiative.

1. Vessel and Port Security

Every commercial vessel arriving at a U.S. port and every U.S. port facility needs to have an approved security plan overseen by the Coast Guard.

Every port facility that a liner vessel (or any other SOLAS regulated, large oceangoing commercial ship) calls must operate pursuant to an approved security plan under the ISPS Code. In the U.S. those plans are approved and overseen by the Coast Guard. In foreign jurisdictions, those plans are approved by the port state's national government and then reviewed and visited by the Coast Guard pursuant to its International Port Security Program, which monitors foreign state compliance with the ISPS Code. Vessels calling at ports that the USCG puts on a non-compliance list must operate at a higher security level and face a greater chance of being inspected upon arrival in the U.S.

Each arriving vessel must provide the Coast Guard with an advance electronic notice of arrival 96 hours prior to arriving at a U.S. port, including a list of all crew members and passengers aboard – each of whom must be a U.S. seaman with a Transportation Worker Identification Credential (TWIC) or must have a U.S. visa in order to get off the ship in a U.S. port.

The Long Range Identification and Tracking (LRIT) system provides the Coast Guard with enhanced visibility (including vessel identity, position, date and time) for ships intending to enter the U.S., and ships passing within 1000 miles of the United States.

The USCG performs safety and security compliance boardings on all U.S. flag vessels and performs "port state control" boardings on non-U.S. flag vessels to ensure compliance with applicable U.S. and international safety and security requirements.

The liner shipping industry's operations are consistent and repetitive – its vessel services and crews call at the same ports every week. So long as there is consistent and professional implementation of the security rules, which is usually a hallmark of the Coast Guard, liner shipping has found little problem in operating in the new vessel or port security environment.

We also appreciate the Coast Guard Commandant's admonition that the "concept of maritime security cannot be reduced to a single threat vector". There are numerous security

risks in the maritime environment that don't involve cargo containers. For example, merchant vessels are defenseless against small boat attacks. We fully support the Coast Guard in its efforts to secure an enormous Maritime Domain against a variety of risks.

The Subcommittee has expressed interest in the cost to industry in establishing, implementing and renewing these MTSA vessel and port facility security plans. When the Coast Guard promulgated its maritime security regulations in 2003 implementing MTSA, it projected that the cost of compliance for the industry would be \$7.331 billion over 10 years.³ We do not have ocean carriers' cost estimates of MTSA plan implementation, because carriers do not account for these costs according to a particular federal statute that required them and because there are a variety of maritime security costs that arise from a variety of security and regulatory measures. What we can say, however, is that Coast Guard enforcement of the MTSA regime is generally reasonable and professional and that the costs are generally seen as acceptable.

2. Personnel Security

As mentioned above, ships bound for the United States file their complete vessel crew and passenger manifest lists to the Coast Guard 96 hours prior to arrival in their electronic notices of arrival. The Coast Guard shares this crew and passenger manifest data with its partner agency, CBP, so that CBP can perform its necessary immigration and background checks without requiring the ship to provide the information separately to CBP. To get off the ship in the United States, seafarers who are not U.S. citizens must obtain U.S. visas and U.S. seafarers must present a Transportation Worker Identification Credential (TWIC).

The Council has supported the TWIC program, mandated by Congress and now being implemented in the maritime sector by the Coast Guard and the Transportation Security Administration (TSA), to credential workers requiring unescorted access to secure areas of maritime facilities. The industry's primary concern has been that the security enhancements envisioned in this new system not pose unreasonable costs or undue impacts on those personnel who work in port terminals on port operations or servicing vessels. The main challenges facing the Coast Guard and TSA as this program matures are: managing the large number of card renewals that are coming due, and implementing the long-awaited TWIC reader technology in U.S. port facilities to finally make use of the biometric technology present in each TWIC card.

³ First year estimated cost of implementation was approximately \$1.5 billion, with an annual cost of approximately \$884 million. Implementation of National Maritime Security Initiatives, 68 Fed.Reg. 60448, 60464 (Oct. 22, 2003).

3. Cargo and Supply Chain Security

The nation's maritime and cargo security regime has been developed under several statutes in addition to MTSA. In particular, following the implementation in early 2002 of the "24 Hour Rule" whereby ocean carriers and NVOCCs must submit pre-loading advance cargo manifest filings, enhancement of containerized cargo screening by CBP was directed by the SAFE Port Act. The Act required: "the electronic transmission to the Department of additional data elements for improved high-risk targeting, including appropriate elements of entry data ... to be provided as advanced information with respect to cargo destined for importation into the United States *prior to loading of such cargo on vessels at foreign ports.*" Pursuant to this mandate, CBP requires U.S. importers or cargo owners to file ten additional cargo data elements with CBP 24 hours prior to vessel loading, and also requires ocean carriers to provide two additional sources of operational data -- vessel stowage plans prior to arrival in the U.S., as well copies of electronic container status messages. This "10 plus 2" initiative substantially improved cargo risk assessment and screening. CBP's strategy has been to require the submission of extensive information about import cargo shipments, from the party having the most direct knowledge of that information, as early in the movement of those goods as is practical. This information is then utilized in the cargo risk screening processes performed by the National Targeting Center on all U.S. bound containerized cargo shipments.

Specifically, CBP's advance cargo security screening program contains the following components:

- 24 hours prior to vessel loading in a foreign port, ocean carriers must provide CBP with the shipping manifest information for all shipments.
- 24 hours prior to vessel loading in a foreign port, non-vessel operating common carriers (NVOCCs) are required to provide CBP with their shipping manifest information for all their shipments.
- 24 hours prior to vessel loading in a foreign port, U.S. importers must provide CBP an Importer Security Filing (ISF). The ISF requires ten data elements for each import shipment; eight of those must be provided 24 hours prior to vessel loading in a foreign port, and two may be provided no later than 24 hours prior to arrival in the U.S. The ISF allows CBP to risk-screen cargo with much more accurate and detailed shipment information -- such as, who is buying the goods, who is selling the goods, where the container was stuffed, who manufactured the goods, country of origin of the goods, the name of consolidator (if applicable).

- Ocean carriers must provide CBP with copies of all their electronic “container status messages” recording various operational events that occurred to containers during their transit, including their time and date.
- Ocean carriers must provide CBP with a copy of the vessel stowage plan no later than 48 hours after vessel departure. The stowage plan shows the stowage location of every container aboard the vessel, and also allows CBP to check to make sure that there are no containers aboard for which there is not the required manifest or ISF data.
- CBP screens the advance manifest and importer data and may issue a “Do Not Load” message or inspect the cargo in cooperation with foreign customs authorities (Container Security Initiative) if CBP has questions about the cargo.
- CBP works with ocean carriers to obtain more information prior to vessel arrival in the U.S. if they have any questions about a container on a vessel.
- CBP inspects all containers judged to be “high risk” by the National Targeting Center.
- CBP performs radiation scanning of all U.S. import containers at U.S. discharge ports.
- Shippers may improve their “risk profile” with CBP by participating in Customs’ Trade Partnership Against Terrorism (C-TPAT).

This is without question the most detailed and extensive advance cargo security screening program in any trading nation. This also is the most detailed advance cargo screening program used by the U.S. government for any transportation mode. We recognize that this regime has been developed under authorities that go beyond MTSA, but discuss it in this testimony because the issue of containerized cargo security has over the years been one of significant interest to the Congress.

The World Shipping Council and its member ocean carriers have supported CBP every step of the way in developing this regime. The reason for our support is straightforward: advance cargo risk assessment is the most prudent and effective approach the U.S. government can take with respect to supply chain security, and for that approach to be effective the government needs sufficient data to be confident of the system’s value and effectiveness. This regime has admittedly added additional processes and cost to shippers and carriers and the government, but we believe it has provided value and has been able to enhance the security of the nation’s supply chains without imposing unreasonable delays or creating inefficiencies in the movement of the nation’s commerce. WSC continues to be ready to work with CBP and the Coast Guard on ways to enhance cargo and supply chain security in an efficient and effective manner.

An example of such cooperation and support to improve the quality and accuracy of the information provided to DHS is the proposal that WSC, the U.S. government, and other

international maritime organizations and governments have made to the International Maritime Organizations (IMO) to amend the Safety of Life at Sea Convention to require that every loaded container be weighed prior to stowage onto a vessel for export.⁴ The safety and security of container operations would be improved by an effective international requirement that the weight of all loaded containers be verified before being loaded onto ships for export. Members of this Subcommittee expressed interest in and support for this idea at the Subcommittee's April 26 hearing on "Regulation of the Maritime Industry". In the United States, container weighing is already required for export containers, pursuant to OSHA regulations. The problem is that most nations of the world do not have such requirements, and therefore ocean carriers routinely have containers loaded aboard their vessels that have not been weighed. In such circumstances, the carrier relies on the declared weight provided by the shipper of the goods, but too often that declaration is not accurate. Sometimes it is grossly inaccurate. This can lead to a host of issues, ranging from safety risks for the vessel and crew and longshore workers, to operational problems for the ship, to collapsed container stacks and containers going overboard, to overweight boxes being unloaded and driven from the discharge port onto local roads. It is a problem that needs to be remedied. For example, if a shipper has declared a container weighs 10 tons, but in reality it weighs 20 tons, there are clearly reasons for both carriers and the government to have concerns. While this initiative is admittedly designed primarily to improve *safety* in the industry, CBP has confirmed that having the verified, actual cargo weights would be helpful to its cargo risk screening activities, including security screening. The IMO will be considering this proposal later this month.

Conclusion

Vigilance against security risks requires the development and implementation of prudent security measures, and the continuing enhancement of such measures as the risks change and take new forms.

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

⁴ This proposal to the IMO is cosponsored by the governments of Denmark, The Netherlands, and the United States, and by the following international maritime organizations with observer status at the IMO: BIMCO, the International Association of Ports and Harbors, International Chamber of Shipping, the International Transport Workers' Federation, and the World Shipping Council.

There will continue to be ways that the current regime can be enhanced. Some of the challenges will be easier to address than others. For example, the challenge of preventing small boats from being used by terrorists to attack critical infrastructure is a daunting one. Another example would be that, while we completely support the expressed policy of the government that it will not shut down its ports or the continued flow of commerce if there were a terrorist attack in the maritime environment, we have little insight into how it would accomplish this important objective.

We believe that the U.S. Coast Guard and CBP do an excellent job trying to address the complex maritime and cargo security challenges. The U.S. government has created the most sophisticated maritime vessel, port, and personnel security regime of any trading nation, and it has done so without unduly disrupting the efficient flow of its commerce and without imposing unacceptable costs on industry participants. The interests of the maritime industry and the government are basically the same: to ensure a safe, secure, and efficient maritime transportation system. We appreciate this Subcommittee's continued interest and oversight of these issues. We would be pleased to provide additional information that may be of assistance. Thank you again for the opportunity to testify.

###

Statement for the Record

Tenth Anniversary of the Maritime Transportation Security Act:
Are We Safer?

Subcommittee on Coast Guard and Maritime Transportation
Committee on Transportation and Infrastructure
U.S. House of Representatives

September 11, 2012

Passenger Vessel Association
103 Oronoco Street, Suite 200
Alexandria, VA 22314
Phone: 703-518-5005
Email: ewelch@passengervessel.com
Web page: www.passengervessel.com

Mr. Chairman and Members of the Subcommittee:

November 25 of this year will mark the 10-year anniversary of enactment of the Maritime Security Act (MTSA) of 2002 (Public Law 107-295). The Committee's hearing asks "Are we safer?" In response, the Passenger Vessel Association (PVA) reports that the domestic U.S.-flagged passenger vessel industry is indeed safe and that we have met all of the mandates of MTSA.

The Passenger Vessel Association is the national trade association representing owners and operators of U.S.-flagged passenger vessels of all types. It represents the interests of owners and operators of dinner cruise vessels, sightseeing and excursion vessels, passenger and vehicular ferries, private charter vessels, whalewatching and eco-tour operators, windjammers, gaming vessels, amphibious vehicles, water taxis, and overnight cruise ships. PVA has been in operation for more than 40 years. PVA currently has about 550 vessel and associate members. Its vessel-operating members range from small family businesses with a single boat to companies with several large vessels in different cities to governmental agencies operating ferries.

Here is a summary of our PVA's points:

- MTSA affects U.S.-flagged vessels and U.S. mariners as much as, if not more than, it does foreign-flagged vessels and foreign seafarers. Congress should carefully consider whether MTSA unnecessarily disadvantages the domestic U.S. maritime industry.

- The U.S.-flagged passenger vessel industry rapidly complied with the mandates and deadlines established by MTSA.
- The Passenger Vessel Association's Coast Guard-approved Alternative Security Program is highly effective in enabling domestic passenger vessels to comply with the MTSA requirement for vessel and security plans.
- For the U.S.-flagged passenger vessel sector, the Transportation Worker Identification Credential (TWIC) has shown itself to be ineffective in promoting security and highly burdensome to passenger vessel operators and U.S. mariners.
- After almost two years, the Department of Homeland Security has failed even to initiate a rulemaking to implement section 809 of the Coast Guard Authorization Act of 2010 providing TWIC relief to certain U.S. citizen mariners.
- TWIC readers are not necessary to ensure security on U.S. passenger vessels. Mandating them for this sector would impose an expensive burden, interfere with day-to-day operations, and fail to provide additional security.
- The use of trained dogs is an effective means of detecting bombs and unauthorized devices on passenger vessels. The federal port security grant program and other aid from the Transportation Security Administration should be made available to passenger vessel operators to contract with companies that provide trained dogs and their handlers.

MTSA affects U.S.-flagged vessels and U.S. mariners as much as, if not more than, it does foreign-flagged vessels and foreign seafarers. Congress should carefully consider whether MTSA unnecessarily disadvantages the domestic U.S. maritime industry.

It is ships in international commerce (primarily those flying foreign flags and carrying foreign seafarers) that pose the threat of introducing nuclear materials or weapons of mass destruction into the U.S. from abroad. Foreign vessels in international trade are the ones that pose the risk of introducing stowaways or unauthorized crew members into the U.S. in violation of our immigration laws.

Given that the greatest threats are associated with foreign vessels in international trade, it is ironic that key parts of MTSA apply to the U.S. fleet (and especially to the U.S. domestic fleet, including passenger vessels), not to foreign ships that come to America. U.S. citizens (not foreign seafarers) are the ones who must obtain the Transportation Worker Identification Credential (TWIC). Selected U.S. vessels (including domestic passenger vessels) are the ones mandated by MTSA to have Coast Guard-approved Vessel Security Plans.

The U.S.-flagged passenger vessel industry rapidly complied with the mandates and deadlines established by MTSA.

Within days after the terrorist attacks of September 11, the Passenger Vessel Association developed and provided to its members interim guidance for enhancing security on their vessels. Subsequently, PVA completed and obtained Coast

Guard approval for the comprehensive *PVA Industry Standard for Security of Passenger Vessels and Small Passenger Vessels and their Facilities*. This Alternative Security Program enables PVA members to meet their MTSA security mandates. As of the summer of 2004 (and in compliance with the regulatory schedule established by MTSA and its implementing regulations), U.S. passenger vessels authorized to carry 150 passengers or more (and those authorized to carry 50 or more on overnight voyages) put in place MTSA-mandated vessel security plans and facility security plans. Hundreds of thousands of U.S. citizen mariners, including crew members of U.S. passenger vessels, obtained TWICs. U.S. passenger vessel companies spent millions of dollars (most of which was NOT offset by federal port security grants) on developing required security plans, hiring and training security staff, and purchasing and installing extra lights, fencing, communications equipment, and closed circuit cameras.

The PVA Alternative Security Program is highly effective in enabling domestic passenger vessels to comply with the MTSA requirement for vessel and security plans.

Currently, approximately 550 vessels in the U.S. domestic passenger vessel sector use the *PVA Industry Standard for Security of Passenger Vessels and Small Passenger Vessels and their Facilities*. This extensive document was developed by PVA members and staff in cooperation with representatives of the U.S. Coast Guard. It has been approved by the Coast Guard and is regularly monitored and periodically revised with Coast Guard acquiescence to take into account new regulatory expectations and lessons learned as it has been implemented

over time. It is referenced specifically in the *U.S. Code of Federal Regulations* as an approved method by which a U.S.-flagged passenger vessel in domestic service can comply with MTSA requirements for vessel and facility security plans. It can be used by any member of PVA in good standing. In addition to helping passenger vessel operators, it also assists the Coast Guard to maximize its internal resources by enabling it to approve a single document rather than hundreds of individually-developed security plans from the passenger vessel sector.

The PVA Alternative Security Program is the most effective MTSA-mandated measure for the passenger vessel sector and is a key reason as to why PVA and the Coast Guard are confident that passenger vessel maritime security remains at a high level, as desired by Congress.

For the U.S.-flagged passenger vessel sector, the Transportation Worker Identification Credential (TWIC) has shown itself to be ineffective in promoting security and highly burdensome to passenger vessel operators and U.S. mariners.

The concept of TWIC may have seemed like a good idea in 2002 when Congress enacted MTSA, but a decade of experience with it has uncovered numerous shortcomings.

Unlike facilities such as container ports, domestic passenger vessels do not have hundreds or thousands of persons who need to enter secure spaces. The number of crew members on a typical U.S.-flagged passenger vessel consists of just a few individuals.

In addition, most U.S. passenger vessels are operated by small companies or small entities, often in areas far removed from a traditional port. Crew members are individually known to and recognized by management, as well as to other crew members. It is not necessary to have TWICs for identity purposes. If you ask the typical passenger vessel operator, he or she will say, "I know my people on sight, and they know one another. We can immediately tell if an unauthorized person tries to gain access. We don't need a TWIC to do that for us."

Obtaining a TWIC is unnecessarily burdensome for many persons. These individuals must endure two separate trips to a TWIC enrollment center (often located many hours away); they also must incur the costs of the TWIC enrollment fee of \$132, travel and overnight lodging costs, and lost wages for time off. The passenger vessel sector has found that, in reality, the employer must bear these expenses or reimburse the employee for them. This is necessary to stay competitive in obtaining qualified labor, because the worker is likely to wish to avoid these costs altogether by seeking non-maritime employment.

PVA acknowledges that the House of Representatives has passed legislation to get rid of the "two trips to the enrollment center" requirement, but prospects for this legislation in the Senate are uncertain, given the relatively few weeks remaining in the 112th Congress.

TWICs may be useful in some parts of the maritime industry (perhaps large port complexes and huge refineries

located on waterfronts), but they are burdensome and ineffective for the domestic passenger vessel sector.

After more than two years, the Department of Homeland Security has failed even to initiate a rulemaking to implement section 809 of the Coast Guard Authorization Act of 2010 providing TWIC relief to certain U.S. citizen mariners.

MTSA originally required every U.S. mariner who holds a valid Coast Guard license or merchant mariner's document to qualify for, pay for, and hold a TWIC. This mandate applied even to a mariner who did not work on a vessel required to have a Coast Guard-approved vessel security plan or one who did work on a security plan vessel but who did not have the privilege of unescorted access to a designated secure area of such a vessel.

Section 809 of Public Law 111-281 changed the TWIC requirement so that it is mandatory only in the case of a U.S. mariner who requires unescorted access to a secure area of a vessel with an approved security plan. As a result of the 2010 law, other mariners now have the individual choice as to whether to obtain or renew a TWIC. This change in law in no way reduced security of U.S.-flagged vessels, but it was an important step in relieving an unnecessary burden for individual U.S. citizen-mariners and their employers.

Unfortunately, the Coast Guard has determined that it will require a rulemaking to implement section 809 fully. Despite the passage of 23 months from enactment of the 2010 law, the

Department of Homeland Security has failed to even issue a proposed rule. In the meantime, confusion is rampant, and mariners who could take advantage of the change in law are still having to apply for TWICs and pay an excessive sum when they do so. PVA asks this Committee to see that the Department of Homeland Security prioritizes the implementation of section 809.

TWIC readers are not necessary to ensure security on U.S. passenger vessels. Mandating them for this sector would impose an expensive burden, interfere with day-to-day operations, and fail to provide additional security.

For many types of vessels and maritime facilities, security dictates that access by members of the public be prohibited or severely curtailed. This is not true of the U.S. passenger vessel sector. Passenger vessels depend on easy access for commuters, customers, and visitors. Ferries adhere to tight schedules, carry tens of thousands of riders each day, and function as forms of mass transit. Dinner boats and sightseeing vessels must attract paying customers and compete with their equivalent shoreside venues (hotels, restaurants, tour busses, etc.). Even if a passenger vessel is required to have a Coast Guard-approved vessel security plan, most parts of the vessel have to be open to members of the public. In other words, the whole vessel itself is not designated as a secure area to which access must be controlled.

Most U.S. passenger vessels are operated by small companies or small entities. Crew members are individually known to and recognized by management, as well as to other

crew members. It is not necessary to have TWICs for identity purposes, and no reason would be served by the installation of TWIC readers.

Three PVA members participated in the Transportation Security Administration's TWIC reader pilot program. These included the Staten Island Ferry, a sightseeing boat company in Annapolis, and a high-speed ferry in Puget Sound. All three operators reported that they derived no security enhancements because of the TWIC readers. To the contrary, the readers retarded normal vessel operations and frequently malfunctioned. TWIC readers may be appropriate for some types of vessels and facilities, but not for U.S. domestic passenger vessels. The TWIC program itself has been a burden on the passenger vessel sector. Imposing a TWIC reader requirement would be infinitely worse.

Trained dogs are an effective means of detecting bombs and unauthorized devices on passenger vessels. The federal port security grant program and other aid from the Transportation Security Administration should be made available to passenger vessel operators to contract with companies that provide trained dogs and their handlers.

Some PVA members have successfully sought federal port security grants to purchase and install physical security features (lights, cameras, fencing, etc.) for their vessels and terminals. However, vessel operators say that trained dogs are the most effective way of enhancing the screening of passengers and vehicles. Unfortunately, for many years eligibility restrictions for port security grants were so onerous that they could not be

used to contract for the use of trained dogs. These restrictions have relaxed somewhat recently, but the Department of Homeland Security should ensure that all of its financial assistance programs can be used easily by vessel operators to procure the services of trained dogs. There is no better way to enhance screening for ferries and other passenger vessels. If maritime security is the government's goal, it should promote the use of dogs for screening.