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 10 Years after the Maritime Transportation Security Act

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

September 11, 2012

MARITIME SECURITY

Progress and Challenges 10 Years After the Maritime Transportation Security Act

GAO Accountability * Integrity * Reliability

Highlights

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

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 obligated 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 August 2002 through July 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

[1]Pub. L. No. 107-295, 116 Stat. 2064.

[2]Immigration 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.

[3]Maritime 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

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

[9]Department 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

[14]GAO, *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 MTSA was 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 MTSA-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] MTSA 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

[15]46 U.S.C. § 70105.

[16]GAO, *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).

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

[18]46 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

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

[20]46 U.S.C. § 70103(c)

[21]GAO, *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

[22]GAO, *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).

[24]The 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

[25]GAO-08-126T.

[26]GAO, *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

[27]See 6 U.S.C. § 943(b).

[28]Importer 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).

[29]GAO, *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

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

[31]GAO, *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 program[32]—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

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

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

[34]CBP 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

[36]The 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.

[37]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. 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

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

[39]GAO, *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).

[40]GAO, *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

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

[42]GAO, *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.

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

[44]GAO, *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

[45]GAO, *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

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

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

[48]GAO, *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts*, GAO-05-557 (Washington, D.C.: Apr. 26, 2005).

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.

[49]GAO-12-14.

[50] GAO-08-12.

[51]GAO-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

[52]The 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).

[53]Illegal 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).

[54]GAO, *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).

[55]GAO, *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.

[58]GAO-12-14.

[59]GAO-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.

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

	Fiscal year[a]									
Funding	**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.

[a]Budget 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, MTSA 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 MTSA (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)

	Fiscal year									
PSGP	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**[d]

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

[a]Target funding amounts as presented in FEMA's annual grant guidance.

[b]This 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.

[c]This figure includes fiscal year 2007 appropriations , as well as $110 million in fiscal year 2007 supplemental appropriation.

[d]Total 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)

	Fiscal year									
TWIC	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.
[a]Funding 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 Works 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, 2989 (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 MTSA. 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 implemented 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)

	Fiscal year							
ATS	2005	2006	2007	2008	2009	2010	2011	2012[a]
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.

[a]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 Oceangoing 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 [a]	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,

[a]We were unable to distinguish between CSI and SFI obligations because they are funded out of the same budget line item.
[b]Represents 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

[a]Expenditures 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)

	Fiscal year								
C-TPAT	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.

[a]Represents 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 multi-faceted 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 or 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, Allyson Goldstein, Paul Hobart, Amanda Kolling, Glen Levis, and Edwin Woodward. Additional contributors include Frances Cook, Tracey King, and Jessica Orr.