United States Government Accountability Office

GAO

Testimony before the Committee on Commerce, Science, and Transportation U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, October 4, 2007

MARITIME SECURITY

The SAFE Port Act and Efforts to Secure Our Nation's Seaports

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

October 4, 2007

MARITIME SECURITY

The SAFE Port Act and Efforts to Secure Our Nation's Seaports

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-86T, a testimony before the Committee on Commerce, Science and Transportation, U.S. Senate

Why GAO Did This Study

Because the safety and economic security of the United States depend in substantial part on the security of its 361 seaports, the United States has a vital national interest in maritime security.
The Security and Accountability for Every Port Act (SAFE Port Act), modified existing legislation and created and codified new programs related to maritime security. The Department of Homeland Security (DHS) and its U.S Coast Guard, Transportation Security Agency, and U.S. Customs and Border Protection have key maritime security responsibilities.
This testimony synthesizes the results of GAO's completed work and preliminary observations from GAO's ongoing work pertaining to overall port security, security at individual facilities, and cargo container security.
To perform this work GAO visited domestic and overseas ports; reviewed agency program documents, port security plans, and post-exercise reports; and interviewed officials from the federal, state, local, private, and international sectors.

What GAO Recommends

GAO has made recommendations to DHS to develop strategic plans, better plan the use of its human capital, establish performance measures, and otherwise improve program operations. DHS has generally concurred with our recommendations and is making progress implementing them. We provided a draft of this testimony to DHS agencies and incorporated technical comments as appropriate.

To view the full product, including the scope and methodology, click on GAO-08-86T. For more information, contact Stephen Caldwell (202) 512- 9610 or caldwells@gao.gov.

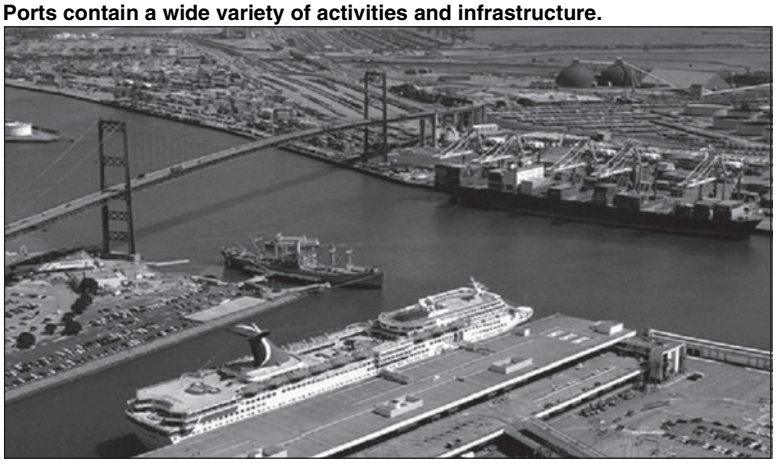
What GAO Found

Federal agencies have improved overall port security efforts by establishing committees to share information with local port stakeholders, and taking steps to establish interagency operations centers to monitor port activities, conducting operations such as harbor patrols and vessel escorts, writing port-level plans to prevent and respond to terrorist attacks, testing such plans through exercises, and assessing the security at foreign ports. However, these agencies face resource constraints and other challenges trying to meet the SAFE Port Act's requirements to expand these activities. For example, the Coast Guard faces budget constraints in trying to expand its current command centers and include other agencies at the centers.

Similarly, private facilities and federal agencies have taken action to improve the security at approximately 3,000 individual facilities by writing facility-specific security plans, and inspecting facilities to make sure they are complying with their plans, and developing special identification cards for workers to prevent terrorist from getting access to secure areas. Again, federal agencies face challenges trying to meet the act's requirements to expand the scope or speed the implementation of such activities. For example, the Transportation Security Agency missed the act's July 2007 deadline to implement the identification card program at 10 selected ports because of delays in testing equipment and procedures.

Federal programs related to the security of cargo containers have also improved as agencies are enhancing systems to identify high-risk cargo, expanding partnerships with other countries to screen containers before they depart for the United States, and working with international organizations to develop a global framework for container security. Federal agencies face challenges implementing container security aspects of the SAFE Port Act and other legislation. For example, Customs and Border Protection must test and implement a new program to screen 100 percent of all incoming containers overseas—a departure from its existing risk-based programs.

Ports contain a wide variety of activities and infrastructure.



Source: United States Coast Guard.

Mr. Chairman and Members of the Committee:

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

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

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

[1]Pub. L. No. 109-347, 120 Stat. 1884 (2006).

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

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

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

[3] The Implementing Recommendations of the 9/11 Commission Act of 2007 amended a SAFE Port Act provision on scanning all United States bound containers at foreign ports. See Pub. L. No. 110-53, §1701(a), 121 Stat. 266, 489-90. This amendment is discussed later in this testimony.

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

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

Source: GAO.

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

- programs related to overall port security, such as those for coordinating among stakeholders, conducting security operations, developing security plans, and conducting exercises to test security procedures;

- programs related specifically to security at individual facilities, such as examining security measures and ensuring that only properly cleared individuals have access to port areas; and,

- programs related specifically to the international supply chain and to cargo container security, such as screening containers at ports both here and abroad and forming partnerships with the private sector.

This statement is based primarily on a body of work we completed in response to congressional requests and mandates for analysis of maritime, port, and cargo security efforts of the federal government.[4] In some cases, we provide preliminary observations from our ongoing work. Thus, the timeliness of the data that were the basis for our prior reporting varies depending on when our products were issued and the preliminary observations are subject to change as we complete our work.

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

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

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

Summary

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

Regarding security at approximately 3000 individual facilities, again federal agencies and the facilities themselves have taken positive steps. In line with MTSA, facilities have written and implemented security plans and the Coast Guard has generally inspected such facilities to verify compliance and take enforcement actions where necessary. The SAFE

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

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

Regarding the security of cargo containers—which carry a large volume of the world's commerce through our ports—CBP has developed a layered security strategy to identify and inspect containers that may contain terrorist weapons of mass destruction. CBP has refined its Automated Targeting System (ATS) to better analyze shipping information and identify suspicious containers, though it does not have the most up to date information for certain containers—that transit beyond the ports as part of the in-bond system, which allows goods to transit the United States without officially entering U.S. commerce. CBP has expanded and improved the management of its Container Security Initiative (CSI) where the agency places U.S. customs officials in foreign ports to help target and inspect suspicious containers. Similarly, CBP has expanded and improved the management of its Customs-Trade Partnership Against Terrorism (C-TPAT) where private companies agree to improve the security of their supply chains in exchange for reduced scrutiny over their shipments. The SAFE Port Act codified these two programs into law and required enhanced management and oversight of these programs. CBP is working to meet these new requirements, but our prior and ongoing work suggest that it may face challenges setting equipment standards and conducting validations of company practices. The Department of Energy (DOE) is

expanding its Megaports program that complements CSI by providing foreign nations with radiation detection equipment to scan containers moving through their ports. The SAFE Port Act also required pilot programs to test new technologies or combine existing technologies to test the feasibility of scanning all U.S.-bound containers overseas. More recent legislation required that all containers bound for the United States be scanned overseas by 2012 with possible extensions for individual ports. Our preliminary observations suggest this requirement potentially creates new challenges for CBP in terms of integrating this with existing programs, working with foreign governments, overcoming logistical barriers, testing new technology, determining resource requirements and responsibilities, and other issues.

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

Prior Actions Have Improved Port Security, but Issues Remain

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

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

currently evaluating the antiterrorism measures maintained at foreign seaports.

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

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

We have previously reported that both of these types of forums have helped foster cooperation and information-sharing.[8] We further reported that AMSCs provided a structure to improve the timeliness, completeness, and usefulness of information sharing between federal and nonfederal stakeholders. These committees improved upon previous information-sharing efforts because they established a formal structure and new procedures for sharing information. In contrast to AMSCs, the Coast Guard's sector command centers can provide continuous information about maritime activities and involve various agencies directly in

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

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

operational decisions using this information. We have reported that these centers have improved information sharing, and the types of information and the way information is shared varies at these centers depending on their purpose and mission, leadership and organization, membership, technology, and resources.

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

[9]According to the Coast Guard, these multiple interagency partners include Customs and Border Protection, Immigration and Customs Enforcement, Department of Defense, the Secure Border Initiative Network (SBInet) Program Office, and State and local partners. A center located in Charleston, South Carolina is managed by the Department of Justice. It was created through an appropriation in the fiscal year 2003 Consolidated Appropriations Resolution (Pub. L. No. 108-7, 117 Stat. 11,53 (2003.)).

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

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

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

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

Operations to Provide Overall Port Security Face Resource Constraints

As part of its operations, the Coast Guard has also imposed additional activities to provide overall port security. The Coast Guard's operations order, Operation Neptune Shield, first released in 2003, specifies the level of security activities to be conducted. The order sets specific activities for each port; however, the amount of each activity is established based on the port's specific security concerns. Some examples of security activities include conducting waterborne security patrols, boarding high-interest vessels, escorting vessels into ports, and enforcing fixed security zones. When a port security level increases, the amount of activity the Coast Guard must conduct also increases.[13] The Coast Guard uses monthly field unit reports to indicate how many of its security activities it is able to perform. Our review of these field unit reports indicates that many ports are having difficulty meeting their port security responsibilities, with resource constraints being a major factor. In an effort to meet more of its security requirements, the Coast Guard uses a strategy that includes partnering with other government agencies, adjusting its activity requirements, and acquiring resources. Despite these efforts, many ports are still having difficulty meeting their port security requirements. The Coast Guard is currently studying what resources are needed to meet certain aspects of its port security program, but to enhance the effectiveness of its port security operations, a more comprehensive study to determine all additional resources and changes to strategy to meet minimum security requirements may be needed. We will be issuing a report on this issue in the near future.

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

Area plans—another MTSA requirement—and their specific provisions have been specified by regulation and Coast Guard directive. Implementing regulations for MTSA specified that area plans include, among other things, operational and physical security measures in place at the port under different security levels, details of the security incident command and response structure, procedures for responding to security threats including provisions for maintaining operations in the port, and procedures to facilitate the recovery of the marine transportation system after a security incident. A Coast Guard Navigation and Vessel Inspection Circular (NVIC) provided a common template for area plans and specified

[13]The Coast Guard uses a three-tiered system of Maritime Security (MARSEC) levels consistent with DHS's Homeland Security Advisory System (HSAS). MARSEC levels are designed to provide a means to easily communicate pre-planned scalable responses to increased threat levels.

the responsibilities of port stakeholders under them.[14] As of September 2007, 46 area plans are in place at ports around the country. The Coast Guard approved the plans by June 1, 2004, and MTSA requires that they be updated at least every 5 years.

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

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

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

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

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

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

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

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

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

committees and MTSA-required area plans to discuss all-hazards planning. DHS concurred with this recommendation.

Maritime Security Exercises Require a Broader Scope and Participation

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

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

Though we have not specifically examined compliance with these new requirements, our work in examining past exercises suggests that

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

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

The security of domestic ports also depends upon security at foreign ports where cargoes bound for the United States originate. To help secure the overseas supply chain, MTSA required the Coast Guard to develop a program to assess security measures in foreign ports and, among other things, recommend steps necessary to improve security measures in those ports. The Coast Guard established this program, called the International Port Security Program, in April 2004. Under this program, the Coast Guard and host nations review the implementation of security measures in the host nations' ports against established security standards, such as the International Maritime Organization's International Ship and Port Facility Security (ISPS) Code.[20] Coast Guard teams have been established to conduct country visits, discuss security measures implemented, and

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

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

collect and share best practices to help ensure a comprehensive and consistent approach to maritime security in ports worldwide. The conditions of these visits, such as timing and locations, are negotiated between the Coast Guard and the host nation. Coast Guard officials also make annual visits to the countries to obtain additional observations on the implementation of security measures and ensure deficiencies found during the country visits are addressed.[21]

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

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

As of September 2007, the Coast Guard reported that it has visited 109 countries under this program and plans to visit another 29 more by

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

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

March 2008.[23] For the countries for which the Coast Guard has issued a final report, the Coast Guard reported that most had "substantially implemented the security code," while a few countries were found to have not yet implemented the ISPS Code and will be subject to a reassessment or other sanctions. The Coast Guard also found several facilities needing improvements in areas such as access controls, communication devices, fencing, and lighting.

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

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

Reluctance by some countries to allow the Coast Guard to visit their ports due to concerns over sovereignty was another challenge cited by program officials in completing the first round of visits. According to these officials, before permitting Coast Guard officials to visit their ports, some countries insisted on visiting and assessing a sample of U.S. ports. The Coast Guard was able to accommodate their request through the program's reciprocal visit feature in which the Coast Guard hosts foreign delegations to visit

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

U.S. ports and observe ISPS Code implementation in the United States. This subsequently helped gain the cooperation of the countries in hosting a Coast Guard visit to their own ports. However, as they begin to revisit countries as part of the program's next phase, program officials stated that sovereignty concerns may still be an issue. Some countries may be reluctant to host a comprehensive country visit on a recurring basis because they believe the frequency—once every 2 to 3 years—too high. Sovereignty also affects the conditions of the visits, such as timing and locations, because such visits are negotiated between the Coast Guard and the host nation. Thus the Coast Guard team making the visit could be precluded from seeing locations that are not in compliance.

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

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

Port Facility Security Efforts Continue, but Additional Evaluation is Needed

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

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

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

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

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

management of its MTSA facility oversight program, particularly documenting compliance activities.

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

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

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

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

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

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

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

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

The SAFE Port Act required TSA to implement TWIC at the 10 highest-risk ports by July 1, 2007, conduct a pilot program to test TWIC access control technologies in the maritime environment; issue regulations requiring TWIC card readers based on the findings of the pilot; and periodically report to Congress on the status of the program. However, TSA did not meet the July 1 deadline, citing the need to conduct additional testing of the systems and technologies that will be used to enroll the estimated 770,000 workers that will be required to obtain a TWIC card. According to TSA officials, the agency plans to complete this testing and begin enrolling workers at the Port of Wilmington in October 2007, and begin enrolling workers at additional ports soon thereafter. TSA is also in the process of conducting a pilot program to test TWIC access control technologies in the maritime environment that will include a variety of maritime facilities and vessels in multiple geographic locations. According to TSA, the results of the pilot program will help the agency issue future regulations that will require the installation of access control systems necessary to read the TWIC cards.

It is important that TSA establish clear and reasonable time frames for implementing TWIC as the agency begins enrolling workers and issuing TWIC cards in October. TSA could face additional challenges as the TWIC implementation progresses; these include monitoring the effectiveness of contract planning and oversight. TSA has developed a quality assurance surveillance plan with performance metrics that the enrollment contractor

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

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

must meet to receive payment. The agency has also taken steps to strengthen government oversight of the TWIC contract by adding staff with program and contract management expertise. However, the effectiveness of these steps will not be clear until implementation of the TWIC program begins. Ensuring a successful enrollment process for the program presents another challenge. According to TSA, the agency has made communication and coordination top priorities by taking actions such as establishing a TWIC stakeholder communication committee and requiring the enrollment contractor to establish a plan for coordinating and communicating with all stakeholders who will be involved in the program. Finally, TSA will have to address access control technologies to ensure that the program is implemented effectively. It will be important that TSA's TWIC access control technology pilot ensure that these technologies work effectively in the maritime environment before facilities and vessels will be required to implement them.

DHS Working to Coordinate Multiple Background Check Programs for Transportation Workers

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

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

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

In April 2007, we completed a study of DHS background check programs as part of a SAFE Port Act requirement to do so.[32] We found that the six programs we reviewed were conducted independently of one another, collected similar information, and used similar background check processes. Further, each program operated separate enrollment facilities to collect background information and did not share it with the other programs. We also found that DHS did not track the number of workers who, needing multiple credentials, were subjected to multiple background check programs. Because DHS is responsible for a large number of background check programs, we recommended that DHS ensure that its coordination plan includes implementation steps, time frames, and budget requirements; discusses potential costs/benefits of program standardization; and explores options for coordinating and aligning background checks within DHS and other federal agencies.

DHS concurred with our recommendations and continues to take steps—both at the department level and within its various agencies—to consolidate, coordinate, and harmonize such background check

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

[32]The SAFE Port Act required that GAO conduct a study of the background records checks carried out for DHS that are similar to the one required of truck drivers to obtain a hazardous material endorsement. Pub. L. No. 109-347, §105 120 Stat. 1884, 1891 (2006). See GAO, *Transportation Security: Efforts to Eliminate Redundant Background Check Investigations*, GAO-07-756 (Washington, D.C.: Apr. 26, 2007).

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

- Credentialing framework: A framework completed in July 2007 that describes a credentialing life-cycle of registration and enrollment, eligibility vetting and risk assessment, issuance, expiration and revocation, and redress. This framework was to incorporate risk-based levels or criteria, and an assessment of the legal, privacy, policy, operational, and technical challenges.

- Technical review: An assessment scheduled for completion in October 2007 is to be completed by the contractor in conjunction with the DHS Office of the Chief Information Officer. This is to include a review of the issues present in the current technical environment and the proposed future technical environment needed to address those issues, and provide recommendations for targeted investment reuse and key target technologies.

- Transition plan: A plan scheduled to be completed in November 2007 is to outline the projects needed to actualize the framework, including identification of major activities, milestones, and associated timeline and costs.

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

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

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

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

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

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

Management of the Automated Targeting System Has Improved

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

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

manifest information 24 hours prior to a United States-bound sea container being loaded onto a vessel in a foreign port. CBP officers use these scores to help them make decisions on the extent of documentary review or additional inspection as required.

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

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

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

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

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

CBP's in-bond system—which allows goods to transit the United States without officially entering U.S. commerce—must balance the competing goals of providing port security, facilitating trade, and collecting trade revenues. However, we have earlier reported that CBP's management of the system has impeded efforts to manage security risks. Specifically, CBP does not collect detailed information on in-bond cargo at the U.S. port of arrival that could aid in identifying cargo posing a security risk and promote effective use of inspection resources.[38]

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

As discussed earlier in this testimony, CBP uses manifest information it receives on all cargo arriving at U.S. ports (including in-bond cargo) as input for ATS scoring to aid in identifying security risks and setting inspection priorities. For regular cargo, the ATS score is updated with

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

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

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

more detailed information as the cargo makes official entry at the arrival port. For in-bond cargo, the ATS scores generally are not updated until these goods move from the port of arrival to the destination port for official entry into United States commerce, or not updated at all for cargo that is intended to be exported.[41] As a result, in-bond goods might transit the United States without having the most accurate ATS risk score.

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

We earlier recommended that the Commissioner of CBP take action in three areas to improve the management of the in-bond program, which included collecting and using improved information on in-bond shipments to update the ATS score for in-bond movements at the arrival port and enable better informed decisions affecting security, trade and revenue collection.[44] DHS agreed with most of our recommendations.[45] According

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

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

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

[44]GAO-07-561.

to CBP, they are in the process of developing an in-bond weight set to be utilized to further identify cargo posing a security risk. The weight set is being developed based on expert knowledge, analysis of previous in-bond seizures, and creation of rules based on in-bond concepts.

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

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

CPB initiated its CSI program to detect and deter terrorists from smuggling weapons of mass destruction (WMD) via cargo containers before they reach domestic seaports in January 2002. The SAFE Port Act formalized the CSI program into law. Under CSI, foreign governments sign a bilateral agreement with CBP to allow teams of U.S. customs officials to be stationed at foreign seaports to identify cargo container shipments at risk of containing WMD. CBP personnel use automated risk assessment information and intelligence to target to identify those at risk containing WMD. When a shipment is determined to be high risk, CBP officials refer it to host government officials who determine whether to examine the shipment before it leaves their seaport for the United States. In most cases, host government officials honor the U.S. request by examining the referred shipments with nonintrusive inspection equipment and, if they deem necessary, by opening the cargo containers to physically search the

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

contents inside.[46] CBP planned to have a total of 58 seaports by the end of fiscal year 2007.

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

Although CBP's goal is to review information about all U.S.-bound containers at CSI seaports for high-risk contents before the containers depart for the United States, we reported in 2005 that the agency has not been able to place enough staff at some CSI ports to do so.[48] Also, the

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

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

[48]GAO-05-557.

SAFE Port Act required DHS to develop a human capital management plan to determine adequate staffing levels in U.S. and CSI ports. CBP has developed a human capital plan, increased the number of staff at CSI ports, and provided additional support to the deployed CSI staff by using staff in the United States to screen containers for various risk factors and potential inspection. With these additional resources, CBP reports that manifest data for all US-bound container cargo are reviewed using ATS to determine whether the container is at high risk of containing WMD. However, the agency faces challenges in ensuring that optimal numbers of staff are assigned to CSI ports due in part to its reliance on placing staff overseas at CSI ports without systematically determining which functions could be performed overseas and which could be performed domestically.

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

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

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

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

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

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

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

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

[51]GAO-05-405.

measures in place, CBP's efforts have focused on measures regarding program participation and facilitating trade and travel. CBP has not yet developed performance measures for C-TPAT's efforts aimed at ensuring improved supply chain security, which is the program's purpose.

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

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

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

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

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

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

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

The SAFE Framework enhances the CSI program by promoting the implementation of CSI-like customs security practices, including the use of electronic advance information requirements and risk-based targeting, in both CSI and non-CSI ports worldwide. The framework also lays the foundation for mutual recognition, an arrangement whereby one country can attain a certain level of assurance about the customs security standards and practices and business partnership programs of another country. In June 2007, CBP entered into the first mutual recognition

arrangement of a business-to-customs partnership program with the New Zealand Customs Service. This arrangement stipulates that members of one country's business-to-customs program be recognized and receive similar benefits from the customs service of the other country. CBP is pursuing similar arrangements with Jordan and Japan, and is conducting a pilot program with the European Commission to test approaches to achieving mutual recognition and address differences in their respective programs. However, the specific details of how the participating counties' customs officials will implement the mutual recognition arrangement—such as what benefits, if any, should be allotted to members of other countries' C-TPAT like programs—have yet to be determined. As CBP goes forward, it may face challenges in defining the future of its CSI and C-TPAT programs and, more specifically, in managing the implementation of mutual recognition arrangements, including articulating and agreeing to the criteria for accepting another country's program; the specific arrangements for implementation, including the sharing of information; and the actions for verification, enforcement; and, if necessary, termination of the arrangement.

DOE Continues to Expand Its Megaports Program

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

Through August 2007, DOE had completed installation of radiation detection equipment at eight ports: Rotterdam, the Netherlands; Piraeus, Greece; Colombo, Sri Lanka; Algeciras, Spain; Singapore; Freeport, Bahamas; Manila, Philippines; and Antwerp, Belgium (Phase I). Operational testing is under way at four additional ports: Antwerp, Belgium (Phase II); Puerto Cortes, Honduras; Qasim, Pakistan; and Laem Chabang, Thailand. Additionally, DOE has signed agreements to begin work and is in various stages of implementation at ports in 12 other countries, including the United Kingdom, United Arab Emirates/Dubai, Oman, Israel, South Korea, China, Egypt, Jamaica, the Dominican

Republic, Colombia, Panama, and Mexico, as well as Taiwan and Hong Kong. Several of these ports are also part of the Secure Freight Initiative, discussed in the next section. Further, in an effort to expand cooperation, DOE is engaged in negotiations with approximately 20 additional countries in Europe, Asia, the Middle East, and Latin America.

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

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

Secure Freight Initiative Testing Feasibility of Combining Scanning Technologies

The SAFE Port Act required that a pilot program—known as the Secure Freight Initiative (SFI)—be conducted to determine the feasibility of 100 percent scanning of U.S. bound containers. To fulfill this requirement, CBP and DOE jointly announced the formation of SFI in December 2006, as an effort to build upon existing port security measures by enhancing the U.S. government's ability to scan containers for nuclear and radiological

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

materials overseas and better assess the risk of inbound containers. In essence, SFI builds upon the CSI and Megaports programs. The SAFE Port Act specified that new integrated scanning systems that couple nonintrusive imaging equipment and radiation detection equipment must be pilot-tested. It also required that, once fully implemented, the pilot integrated scanning system scan 100 percent of containers destined for the United States that are loaded at pilot program ports.

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

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

New Requirement for 100 Percent Scanning Introduces New Challenges

Recent legislative actions have updated U.S. maritime security requirements and may affect overall international maritime security strategy. In particular, the recently enacted Implementing Recommendations of the 9/11 Commission Act (9/11 Act) requires, by 2012, 100 percent scanning of U.S.-bound cargo containers using nonintrusive imaging equipment and radiation detection equipment at foreign seaports. The act also specifies conditions for potential extensions beyond 2012 if a seaport cannot meet that deadline. Additionally, it requires the Secretary of DHS to develop technological and operational

standards for scanning systems used to conduct 100 percent scanning at foreign seaports. The Secretary also is required to ensure that actions taken under the act do not violate international trade obligations and are consistent with the WCO SAFE Framework. The 9/11 Act provision replaces the requirement of the SAFE Port Act that called for 100 percent scanning of cargo containers before their arrival in the United States, but required implementation as soon as possible rather than specifying a deadline. While we have not yet reviewed the implementation of the 100 percent scanning requirement, we have a number of preliminary observations based on field visits of foreign ports regarding potential challenges CBP may face in implementing this requirement:

- **CBP may face challenges balancing new requirement with current international risk management approach.** CBP may have difficulty requiring 100 percent scanning while also maintaining a risk-based security approach that has been developed with many of its international partners. Currently, under the CSI program, CBP uses automated targeting tools to identify containers that pose a risk for terrorism for further inspection before being placed on vessels bound for the United States. As we have previously reported, using risk management allows for reduction of risk against possible terrorist attack to the nation given resources allocated and is an approach that has been accepted governmentwide. Furthermore, many U.S. and international customs officials we have spoken to, including officials from the World Customs Organization, have stated that the 100 percent scanning requirement is contrary to the SAFE Framework developed and implemented by the international customs community, including CBP. The SAFE Framework, based on CSI and C-TPAT, calls for a risk management approach, whereas the 9/11 Act calls for the scanning of all containers regardless of risk.

- **United States may not be able to reciprocate if other countries request it.** The CSI program, whereby CBP officers are placed at foreign seaports to target cargo bound for the United States, is based on a series of bilateral, reciprocal agreements with foreign governments. These reciprocal agreements also allow foreign governments the opportunity to place customs officials at U.S. seaports and request inspection of cargo containers departing from the United States and bound for their home country. Currently, customs officials from certain countries are stationed at domestic seaports and agency officials have told us that CBP has inspected 100 percent of containers that these officials have requested for inspection. According to CBP officials, the SFI pilot, as an extension of the CSI program, allows foreign officials to ask the United States to reciprocate and scan

100 percent of cargo containers bound for those countries. Although the act establishing the 100 percent scanning requirement does not mention reciprocity, CBP officials have told us that the agency does not have the capacity to reciprocate should it be requested to do so, as other government officials have indicated they might when this provision of the 9/11 Act is in place.

- **Logistical feasibility is unknown and may vary by port.** Many ports may lack the space necessary to install additional equipment needed to comply with the requirement to scan 100 percent of U.S. bound containers. Additionally, we observed that scanning equipment at some seaports is located several miles away from where cargo containers are stored, which may make it time consuming and costly to transport these containers for scanning. Similarly, some seaports are configured in such a way that there are no natural bottlenecks that would allow for equipment to be placed such that all outgoing containers can be scanned and the potential to allow containers to slip by without scanning may be possible. Transshipment cargo containers—containers moved from one vessel to another—are only available for scanning for a short period of time and may be difficult to access. Similarly, it may be difficult to scan cargo containers that remain on board a vessel as it passes through a foreign seaport. CBP officials told us that currently containers such as these that are designated as high-risk at CSI ports are not scanned unless specific threat information is available regarding the cargo in that particular container.

- **Technological maturity is unknown.** Integrated scanning technologies to test the feasibility of scanning 100 percent of U.S. bound cargo containers are not yet operational at all seaports participating in the pilot program, known as SFI. The SAFE Port Act requires CBP to produce a report regarding the program, which will include an evaluation of the effectiveness of scanning equipment at the SFI ports. However, this report will not be due until April 2008. Moreover, agency officials have stated that the amount of bandwidth necessary to transmit scanning equipment outputs to CBP officers for review exceeds what is currently feasible and that the electronic infrastructure necessary to transmit these outputs may be limited at some foreign seaports. Additionally, there are currently no international standards for the technical capabilities of inspection equipment. Agency officials have stated that CBP is not a standard setting organization and has limited authority to implement standards for sovereign foreign governments.

- **Resource responsibilities have not been determined.** The 9/11 Act does not specify who would pay for additional scanning equipment, personnel, computer systems, or infrastructure necessary to establish 100 percent scanning of U.S. bound cargo containers at foreign ports. According to the Congressional Budget Office (CBO) in its analysis of estimates for implementing this requirement, this provision would neither require nor prohibit the U.S. federal government from bearing the cost of conducting scans. For the purposes of its analysis, CBO assumed that the cost of acquiring, installing, and maintaining systems necessary to comply with the 100 percent scanning requirement would be borne by foreign ports to maintain trade with the United States. However, foreign government officials we have spoken to expressed concerns regarding the cost of equipment. They also stated that the process for procuring scanning equipment may take years and can be difficult when trying to comply with changing U.S. requirements. These officials also expressed concern regarding the cost of additional personnel necessary to: (1) operate new scanning equipment; (2) view scanned images and transmit them to the United States; and (3) resolve false alarms. An official from one country with whom we met told us that, while his country does not scan 100 percent of exports, modernizing its customs service to focus more on exports required a 50 percent increase in personnel, and other countries trying to implement the 100 percent scanning requirement would likely have to increase the size of their customs administrations by at least as much.

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

CBP officials have indicated they are aware that challenges exist. They also stated that the SFI will allow the agency to determine whether these challenges can be overcome. According to senior officials from CBP and international organizations we contacted, 100 percent scanning of containers may divert resources, causing containers that are truly high risk to not receive adequate scrutiny due to the sheer volume of scanning outputs that must be analyzed. These officials also expressed concerns

that 100 percent scanning of U.S.-bound containers could hinder trade, leading to long lines and burdens on staff responsible for viewing images. However, given that the SFI pilot program has only recently begun, it is too soon to determine how the 100 percent scanning requirement will be implemented and its overall impact on security.

Agency Comments

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

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

GAO Contact and Staff Acknowledgments

For information about this testimony, please contact Stephen L. Caldwell, Director, Homeland Security and Justice Issues, at (202) 512-9610, or caldwells@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this testimony include Richard Ascarate, Jonathan Bachman, Jason Bair, Fredrick Berry, Christine Broderick, Stockton Butler, Steven Calvo, Frances Cook, Christopher Currie, Anthony DeFrank, Wayne Ekblad, Christine Fossett, Nkenge Gibson, Geoffrey Hamilton, Christopher Hatscher, Valerie Kasindi, Monica Kelly, Ryan Lambert, Nicholas Larson, Daniel Klabunde, Matthew Lee, Gary Malavenda, Robert Rivas, Leslie Sarapu, James Shafer, and April Thompson.

GAO Related Products

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Susan Becker, Acting Manager, BeckerS@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548