United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Border, Maritime, and Global Counterterrorism; Committee on Homeland Security; House of Representatives

For Release on Delivery
Expected at 1:00 p.m. EDT
Thursday, April 26, 2007

MARITIME SECURITY

Observations on Selected Aspects of the SAFE Port Act

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

April 26, 2007

MARITIME SECURITY

Observations on Selected Aspects of the SAFE Port Act

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-754T, a testimony before the Subcommittee on Border, Maritime, and Global Counterterrorism; Committee on Homeland Security; House of Representatives

Why GAO Did This Study

The United States has a vital national interest in maritime security. The safety and economic security of the United States depend in substantial part upon the secure use of the world's waterways and ports. In an effort to further the progress made through the Maritime Transportation Security Act of 2002, the Security and Accountability for Every Port Act (SAFE Port Act) was passed and became effective in October 2006.

This testimony, which is based on past GAO work, synthesizes the results of this work as it pertains to the following:

- overall port security,
- facility security at U.S. ports,
- the international supply chain and cargo container security, and
- customs revenue collection efforts.

What GAO Recommends

While this testimony makes no recommendations, in the past GAO has made many recommendations on issues covered in this statement. The Department of Homeland Security is in various stages of implementing these recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-754T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Stephen L. Caldwell at (202) 512-9610 or CaldwellS@gao.gov. .

What GAO Found

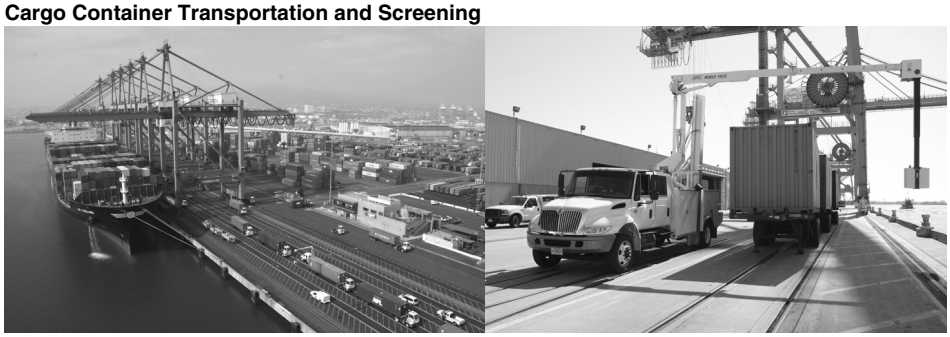
With the Coast Guard generally implementing earlier port security requirements, the SAFE Port Act called for changes to several ongoing programs. For example, it called for interagency operational centers at high-risk ports within 3 years. Three centers currently operate, but agency coordination will pose a challenge. Also, the act established a port security exercise program, but more exercises could challenge stakeholders' ability to maintain coordination and quickly report results. Additionally, an expansion of foreign port security assessments may be challenged by greater workloads and the need for additional staff.

Many port facility security requirements are being implemented, but not always on schedule. While the Coast Guard has approved, and verified through inspection, facility security plans, the SAFE Port Act requires inspections more often and some without notice. The Coast Guard will be challenged by the number of trained inspectors it needs. Worker credentialing programs were also modified by the act. One such program has seen substantial delays in the past, but is receiving more support. Efforts to avoid duplication in these programs will be challenged by the need for extensive coordination within and among federal departments.

The SAFE Port Act codified existing major container security programs and also added guidance for these programs. It also required programs to test new technologies or combine existing technologies for scanning containers. While more container security activity is occurring overseas, challenges remain in the continued implementation of these efforts. These challenges include the inability to directly test the security measures used by different companies in their supply chains, particularly overseas.

Since its formation, the Department of Homeland Security has faced challenges in maintaining its customs revenue functions. For example, the Department failed to maintain the legislatively mandated staffing levels, lacks a strategic workforce plan to help ensure it has a sufficient number of skilled staff to effectively perform customs revenue functions, and CBP does not publicly report on its performance of customs revenue functions, which would help ensure accountability.

Cargo Container Transportation and Screening



Source: CBP.

Madam Chairwoman and Members of the Subcommittee:

I am pleased to be here today to discuss port security and revenue functions related to provisions of the Security and Accountability for Every Port Act (SAFE Port Act).[1] The nation's ports are the doorway for more than 80 percent of our foreign trade. Worldwide, some 30 large ports, spread across North America, Asia, and Europe constitute the world's primary, interdependent trading web. Much of this trade—particularly high-value cargo—enters and leaves in cargo containers. In 2004, for example, $423 billion worth of goods traveling to the United States arrived in 15.8 billion containers. Similarly, ports are vital for our energy supplies. In 2005, 55 percent of the nation's crude oil supply and natural gas supply was imported on seagoing tankers. The trade that passes through ports also generates substantial revenue for the U.S. government.

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

Since the 9/11 attacks, a new port security framework has taken form. Much of this framework was set in place by the Maritime Transportation Security Act (MTSA).[2] Enacted in November 2002, MTSA was designed, in part, to help protect the nation's ports and waterways from terrorist attacks through a wide range of security improvements. Among the major requirements included in MTSA were: (1) conducting vulnerability assessments for port facilities, and vessels.; (2) developing security plans to mitigate identified risks for the national maritime system, ports, port facilities, and vessels; (3) developing the Transportation Worker Identification Credential (TWIC), a biometric identification card to help restrict access to secure areas to only authorized personnel; and (4) establishment of a process to assess foreign ports, from which vessels

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

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

depart on voyages to the United States. Much of this framework is administered by the Department of Homeland Security (DHS), itself a creation of the new security environment brought on by the September 11, 2001, attacks. This framework also attempts to balance security priorities with the need to facilitate legitimate trade.

One of the latest additions to this port security framework is the SAFE Port Act, which was passed and took effect in October of 2006. The act made a number of adjustments to programs within this framework, creating additional programs or lines of effort and altering others. The SAFE Port Act created and codified new programs and initiatives, and amended some of the original provisions of MTSA. The SAFE Port Act included provisions that (1) codified the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT)—two programs administered by Customs and Border Protection (CBP) to help reduce any threats stemming from cargo containers; (2) established port security interagency operational centers at all high risk ports; (3) set an implementation schedule and fee restrictions for TWIC; (4) required that all containers entering high volume U.S. ports be scanned for radiation sources by December 31, 2007; and (5) required additional data be made available to CBP for targeting cargo containers for inspection. The SAFE Port Act also mandated GAO to report to Congress on some topics related to maritime security, including (a) the security of ports overseas in the Caribbean Basin, (b) the background check program for transportation workers, including those seeking access to ports and other sensitive areas, and (c) the extent to which DHS continues to collect revenues at ports given the new emphasis on security.[3] This statement summarizes our work on these three mandates, though all of them have been, or will be, addressed in separate reports.

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

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

Table 1: Summary of Programs and Lines of Effort Included in this Statement

Program	Description
Overall port security	
Area Maritime Security Committees	Committees consisting of key port stakeholders who share information and develop port security plans.
Interagency Operational Centers	Command centers where agencies share information, coordinate their activities, and coordinate joint efforts.
Area Maritime Security Plans	Plan laying out local port vulnerabilities, responsibilities, and some response actions
Port security exercises	Exercises among various port stakeholders to test the effectiveness of port security plans.
Evaluations of security at foreign ports	Coast Guard officers visiting and assessing security conditions at foreign ports.
Port facility security	
Port facility security plans	Facilities are required to have security plans and security officers.
Port facility security compliance monitoring	Coast Guard reviews of port facility security plans and their compliance with such plans.
Transportation Worker Identification Credential	Biometric identification cards to be issued to port workers to help secure access to areas of ports.
Background checks	DHS requirements for person who enter secure or restricted areas or transport hazardous cargo.
International supply chain—container security	
Automated Targeting System	Risk based decision system to determine cargo containers requiring inspection.
Container Security Initiative	Stationing CBP officers at foreign ports to help identify and inspect high risk cargo containers.
Megaports Initiative	Radiation detection technology at foreign ports to stop the proliferation of Weapons of Mass Destruction.
Secure Freight Initiative	Combines Container Security Initiative scanning with Megaports Initiative radiation detection at foreign ports.
Customs-Trade Partnership Against Terrorism	Partnership between private companies and CBP to improved international supply chain security.
Customs revenue functions	
Customs and Border Protection	Collect revenues applied to incoming cargo as appropriate based on tariffs and other laws and regulations.

Source: GAO.

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

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

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

- Programs related more specifically to the international supply chain and to cargo container security, such as screening containers at ports both here and abroad.

- The extent to which DHS—and more specifically, CBP—has maintained the customs revenue function at ports formerly managed by Treasury.

This statement is based primarily on a body of work we have completed in response to congressional requests and mandates for analysis of maritime, port, and cargo security efforts of the federal government. The end of this report has a list of relevant GAO reports and testimonies. As such, the timeliness of the data that was the basis for our prior reporting varies depending on when our products were issued. In several cases, such as CBP's maintenance of effort on the customs revenue function, our findings are based on recent work specifically conducted in response to SAFE Port Act requirements. We conducted all of our work in accordance with generally accepted government auditing standards, and the scope and methodology for this work can be found in the respective products. Similarly, agency comments on the findings we cite can be found in the respective products. While this body of work does not cover all the provisions of the SAFE Port Act, it does cover a wide range of these provisions.

Summary

Regarding overall port security, the Coast Guard has generally implemented key requirements laid out in MTSA. It has established area maritime security committees, written area maritime security plans, conducted exercises to test such plans, and visited foreign ports to assess their compliance with international port security standards. In addition, the SAFE Port Act called for changes in several programs related to developing and testing security plans and coordinating information across agency lines. For example, it called for establishing interagency operational centers at all high-risk ports in the United States within 3 years. Three ports currently have such centers, which are designed to have a unified command structure that can act on a variety of incidents ranging from possible terrorist attacks to search and rescue and environmental response operations. Several new interagency operational centers are about to come on line, but in continuing the expansion, DHS

may face such challenges as creating effective working relationships and dealing with potential coordination problems. Additionally, the SAFE Port Act required the establishment of a Port Security Exercise Program to test and evaluate the capabilities of various governmental and nongovernmental entities when faced with emergencies, and to improve the communication of lessons learned during the exercises. We have not specifically reviewed the implementation of these new requirements, but our past work suggests that the need to increase the already substantial exercise program, the need to quickly and thoroughly complete after action reports and the increased need for interagency coordination for the exercises may challenge port security stakeholders' efforts. The act also called for expanding a program in which the Coast Guard works with other countries to assess—and where needed, strengthen—their security procedures. The Coast Guard has developed plans for meeting these requirements, but it is likely to face challenges in developing sufficient staff to deal with the increased workload.

Regarding security at individual facilities at ports, MTSA has generally been implemented in that facilities have generally written and implemented security plans and the Coast Guard has inspected such facilities to verify compliance and take enforcement actions where necessary. However, the MTSA required transportation worker identification card has been plagued by delays. The SAFE Port Act called for such steps as mandating the frequency of Coast Guard inspections of facilities, requiring unannounced inspections, and directing the implementation of the initial phase of the transportation worker identification credential program by mid-2007. The Coast Guard, which is responsible for the facility inspection program, is likely to face challenges in putting enough trained inspectors in place, especially since many experienced inspectors are scheduled to rotate to other duties. The Transportation Security Administration (TSA), the agency responsible for implementing the identification credential, told us it has drawn up plans and schedules for implementing the program as required and has also brought on additional expertise to deal with past problems in the program's development. The effectiveness of these steps is not likely to be known until the deadlines approach. While DHS has created the Screening Coordination Office to better coordinate the various background checks, it will be challenged to fully coordinate all the DHS screening programs, ensuring that the cost and benefits of potentially eliminating or keeping different screening programs are properly considered, and coordinating with other federal screening programs outside DHS.

Regarding the security of containers that move through ports, CBP has developed a layered security strategy to identify and inspect suspicious containers, and to work with both foreign governments and private firms to improve the security of the international supply chain. Many of the provisions in the SAFE Port Act dealing with container security served to codify existing programs in DHS—such as a program to place CBP officials in foreign ports to help target suspicious containers and a program where private companies agree to improve the security of their supply chains in exchange for reduced scrutiny over their shipments—it also expanded and provided additional guidance for those programs. The SAFE Port Act also required pilot programs to test new technologies or combine existing technologies for inspecting cargo containers. In our prior work on container security programs, we found that progress had been made, but challenges could affect ongoing efforts. Examples of progress made include increasing the number of foreign ports where U.S. officials are located and a rapid growth in the number of companies agreeing to take steps to secure their supply chains. Examples of challenges include ensuring adequate staff are available, and the inability to directly test the security measures used by different companies in their supply chains, particularly overseas.

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

Reports, the official documents agencies issue to Congress and the public to report program performance.

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

Prior Actions Have Improved Port Security, but Challenges Remain

Port security in general has improved as a result of the development of organizations and programs such as Area Maritime Security Committees (area committees), Area Maritime Security Plans (area plans), maritime security exercises, and the International Port Security Program, but challenges to successful implementation of these efforts remain. Additionally, management of these programs will need to address additional requirements directed by the SAFE Port Act. Area committees and interagency operational centers have improved information sharing, but the types and ways information is shared varies. Area plans are limited to security incidents and could benefit from unified planning to include an all-hazards approach. Maritime security exercises would benefit from timely and complete after action reports, increased collaboration across federal agencies, and broader port level coordination. The Coast Guard's International Port Security Program is currently evaluating the antiterrorism measures maintained at foreign seaports.

Area Committees and Interagency Operational Centers Have Become Important Forums for Cooperation and Information-Sharing across Agencies

Two main types of forums have developed as ways for agencies to cooperate and share information about port security—area committees and interagency operational centers. Area committees serve as a forum for port stakeholders, facilitating the 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 area committees—composed of federal, state, local, and industry members—that help to develop the area plan for the port. As of June 2006, the Coast Guard had organized 46 area committees. Each has flexibility to assemble and operate in a way that reflects the needs of its port area, resulting in variations in the number of participants, the types of state and local organizations involved, and the way in which information is shared. Some examples of information shared includes assessments of vulnerabilities at specific port locations, information about potential

threats or suspicious activities, and Coast Guard strategies intended for use in protecting key infrastructure.

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

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

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

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

types of information and the way information is shared varies at the operational centers depending on their purpose and mission, leadership and organization, membership, technology, and resources.

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

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

- **Obtaining security clearances for port security stakeholders.** The lack of federal security clearances among port security stakeholders has been routinely cited as a barrier to information sharing, one of the primary goals of both the area committees and interagency operational centers. In previous reviews, we found that the inability to share classified information may limit the ability to deter, prevent, and respond to a potential terrorist attack. The Coast Guard has seen improvements based on its efforts to sponsor security clearances for members of area committees. In addition, the SAFE Port Act includes a specific provision requiring DHS to sponsor and expedite security clearances for participants in interagency operational centers. However, the extent to which these efforts will ultimately improve information sharing remains unclear.

- **Creating effective working relationships.** Another challenge associated with establishing interagency operational centers at all high risk ports is the difficulty associated with encouraging various federal,

state and local agencies that have never worked together before to collaborate and share information effectively under new structures and procedures. While some of the existing operational centers found success with existing interagency relationships, other high-risk ports might face challenges establishing new working relationships among port stakeholders and implementing their own interagency operational centers.

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

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

Area Plans Are in Place but Do Not Address Natural Disasters

Area plans are another MTSA requirement, and the specific provisions of the plans have been specified by regulation and Coast Guard directive. Implementing regulations for MTSA specified that area plans include, among other things, operational and physical security measures in place at the port under different security levels, details of the security incident command and response structure, procedures for responding to security threats including provisions for maintaining operations in the port, and procedures to facilitate the recovery of the marine transportation system after a security incident. A Coast Guard Navigation and Vessel Inspection Circular (NVIC) provided a common template for area plans and specified the responsibilities of port stakeholders under the plans.[7] Currently, 46 area plans are in place at ports around the country. The Coast Guard

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

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

approved the plans by June 1, 2004, and MTSA requires that they be updated at least every 5 years.

The SAFE Port Act added a requirement to area plans. To ensure that the waterways are cleared and the flow of commerce through United States ports is reestablished as efficiently and quickly as possible after a security incident, the act specified that area plans include a salvage response provision identifying salvage equipment capable of restoring operational trade capacity. None of our past or current work specifically addresses the extent to which area plans now include this provision. We have, however, conducted other work that has a broader bearing on the scope of area plans, and thus potentially on this provision as well.

In a recent report examining how ports are dealing with planning for natural disasters such as hurricanes and earthquakes, we noted that area plans cover security issues but do not include other issues that could have a major impact on a port's ability to support maritime commerce.[8] As currently written, area plans are concerned with deterring and, to a lesser extent, responding to security incidents. We found, however, that unified consideration of all risks faced by a port, both natural and man-made, may be beneficial. Because of the similarities between the consequences of terrorist attacks and natural or accidental disasters, much of the planning for protection, response, and recovery capabilities is similar across all emergency events. Combining terrorism and other threats can enhance the efficiency of port planning efforts because of the similarity in recovery plans for both natural and security-related disasters. This approach also allows port stakeholders to estimate the relative value of different mitigation alternatives. The exclusion of certain risks from consideration, or the separate consideration of a particular type of risk, gives rise to the possibility that risks will not be accurately assessed or compared, and that too many or too few resources will be allocated toward mitigation of a particular risk. As ports continue to revise and improve their planning efforts, available evidence indicates that, if ports take a system-wide approach, thinking strategically about using resources to mitigate and recover from all forms of disaster, they will be able to achieve the most effective results. Area plans provide a useful foundation for establishing an all-hazards approach. While the SAFE Port Act does not call for expanding area plans in this manner, it does contain a requirement that natural

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

disasters and other emergencies be included in the scenarios to be tested in the Port Security Exercise Program. Based on our work, we found there are challenges in using area committees and plans as the basis for broader all-hazards planning. These challenges include:

- **Determining the extent that security plans can serve all-hazards purposes.** We recommended that DHS encourage port stakeholders to use area committees and area plans to discuss all-hazards planning. While MTSA and its implementing regulations are focused on transportation security incidents rather than natural disasters and other types of emergencies, we believe that area plans provide a useful foundation for establishing an all hazards approach. Some federal officials indicated that separate existing plans can handle the range of threats that ports face. However, there would need to be an analysis of gaps between different types of planning. Finally, DHS noted that most emergency planning should properly remain with state and local emergency management planners and were cautious about the federal government taking on a larger role.

Maritime Security Exercises Require a Broader Scope and Participation

MTSA regulations require the Coast Guard Captain of the Port and the area committee to conduct or participate in exercises to test the effectiveness of area plans once each calendar year, with no more than 18 months between exercises. These exercises are designed to continuously improve preparedness by validating information and procedures in the area plan, identifying weaknesses and strengths, and practicing command and control within an incident command/unified command framework. Such exercises have been conducted for the past several years. For example, in fiscal year 2004, the Coast Guard conducted 85 port-based terrorism exercises that addressed a variety of possible scenarios. In August 2005, the Coast Guard and the Transportation Security Administration (TSA) initiated the Port Security Training Exercise Program (PortSTEP)—an exercise program designed to involve the entire port community, including public governmental agencies and private industry, and intended to improve connectivity of various surface transportation modes and enhance area plans. Between August 2005 and October 2007, the Coast Guard expects to conduct PortSTEP exercises for 40 area committees and other port stakeholders.

The SAFE Port Act included several new requirements related to security exercises. It required the establishment of a Port Security Exercise Program to test and evaluate the capabilities of governments and port stakeholders to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism, natural disasters, and other emergencies at

facilities regulated by the MTSA. It also required the establishment of a port security exercise improvement plan process that would identify, disseminate, and monitor the implementation of lessons learned and best practices from port security exercises. Finally, it added natural disasters, such as hurricanes or earthquakes, to be included in the list of scenarios to be tested.

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

- **Setting the scope of the program.** It will be necessary to determine how exercise requirements in the SAFE Port Act differ from area committee exercises that are currently performed. Exercises currently conducted by area committees already test the ability of a variety of port stakeholders to work together in the event of a port incident. The potential exists for these efforts to be duplicated under the SAFE Port Act exercise requirements. On the other hand, the SAFE Port Act exercise requirements clearly move beyond previous requirements by including natural disasters and other emergencies in the list of scenarios to be exercised. Ensuring that these scenarios are exercised as part of a comprehensive security program may require a wider scope when exercise planning commences.

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

- **Ensuring that all relevant agencies participate.** While exercise preparation and participation is time-consuming, joint exercises are

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

necessary to resolve potential role and incident command conflicts as well as determine whether activities would proceed as planned. Our work has shown that past exercises have not necessarily been conducted in this manner.

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

The security of domestic ports is also dependent on security at foreign ports where cargoes bound for the United States originate. To help secure the overseas supply chain, MTSA required the Coast Guard to develop a program to assess security measures in foreign ports and, among other things, recommend steps necessary to improve security measures in their ports. The Coast Guard established this program, called the International Port Security Program, in April 2004. Under this program, the Coast Guard and host nations review the implementation of security measures in the host nations' ports against established security standards, such as the International Maritime Organization's International Ship and Port Facility Security (ISPS) Code.[10] Coast Guard teams have been established to conduct country visits, discuss security measures implemented, and collect and share best practices to help ensure a comprehensive and consistent approach to maritime security in ports worldwide. The conditions of these visits, such as timing and locations, are negotiated between the Coast Guard and the host nation. Coast Guard officials also make annual visits to the countries to obtain additional observations on the implementation of security measures and ensure deficiencies found during the country visits are addressed.[11] As of April 2007, the Coast Guard reported that it has visited 86 countries under this program and plans to complete 29 more visits by the end of fiscal year 2007.[12]

[10]The International Port Security Program uses the ISPS Code as the benchmark by which it measures the effectiveness of a country's anti-terrorism measures in a port. The code was developed after the September 11, 2001, attacks and established measures to enhance the security of ships and port facilities with a standardized and consistent security framework. The ISPS code requires facilities to conduct an assessment to identify threats and vulnerabilities and then develop security plans based on the assessment. The requirements of this code are performance-based; therefore compliance can be achieved through a variety of security measures.

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

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

The SAFE Port Act and other congressional directions have called for the Coast Guard to increase the pace of its visits to foreign countries. Although MTSA did not set a timeframe for completion of these visits, the Coast Guard initially set a goal to visit all countries that conduct maritime trade with the United States by December 2008. In September 2006, the conference report accompanying the fiscal year 2007 DHS Appropriations Act directed the Coast Guard to "double the amount" at which it was conducting its visits.[13] Subsequently, in October 2006, the SAFE Port Act required the Coast Guard to reassess security measures at the foreign ports every 3 years. Coast Guard officials said they will comply with these more stringent requirements and will reassess countries on a 2-year cycle. With the expedited pace, the Coast Guard now expects to assess all countries by March 2008, after which reassessments will begin.

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

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

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

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

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

- **Ensuring sufficient numbers of adequately trained personnel**. Coast Guard officials said the faster rate at which foreign ports will now be reassessed will require hiring and training new staff—a challenge they expect will be made more difficult because experienced personnel who have been with the program since its inception are being transferred to other positions as part of the Coast Guard's rotational policy. These officials will need to be replaced with newly assigned personnel. Another related challenge is that the unique nature of the program requires the Coast Guard to provide specialized training to those joining the program, since very few people in the Coast Guard have had international experience or extensive port security experience.

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

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

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

Coast Guard Faces Challenges in Monitoring Compliance of Maritime Facilities

MTSA and its implementing regulations requires owners and operators of certain at-risk maritime facilities (such as power stations, chemical manufacturing facilities, and refineries that are located on waterways and receive foreign vessels) to conduct assessments of their security vulnerabilities, develop security plans to mitigate these vulnerabilities, and implement measures called for in the security plans. Under the Coast Guard regulations, these plans are to include such items as measures for access control, responses to security threats, and drills and exercises to train staff and test the plan.[16] The plans are "performance-based," meaning the Coast Guard has specified the outcomes it is seeking to achieve and has given facilities responsibility for identifying and delivering the measures needed to achieve these outcomes. Facility owners were to have their plans in place by July 1, 2004.

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

Coast Guard guidance calls for the Coast Guard to conduct on-site facility inspections to verify continued compliance with the plan on an annual basis. The SAFE Port Act required the Coast Guard to conduct at least two inspections of each facility annually, and it required that one of these inspections be unannounced. We are currently conducting a review of the Coast Guard's efforts for ensuring facilities' compliance with various

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

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

MTSA requirements and are not yet in a position to report our findings.[18] However, our previous work showed the Coast Guard faces challenges in carrying out its strategy to review and inspect facilities for compliance with their security plans, and these challenges could be amplified with the additional requirements called for by the SAFE Port Act.[19] These challenges include:

- **Ensuring that sufficient trained inspectors are available.** Because security measures are performance-based, evaluating them involves a great deal of subjectivity. For example, inspectors do not check for compliance with a specific procedure; instead, they have to make a judgment about whether the steps the owner or operator has taken provide adequate security. Performance-based plans provide flexibility to owners and operators, but they also place a premium on the skills and experience of inspectors to identify deficiencies and recommend corrective action. This complexity makes it a challenge for the Coast Guard to ensure that its inspectors are trained appropriately and have sufficient guidance to make difficult judgments about whether owners and operators have taken adequate steps to address vulnerabilities. Additionally, once proficient at their job, inspectors often face reassignment. Further, the rotation period has been shortened by 1 year—from 4 years to 3.

- **Evaluating compliance activities so they can be improved.** In our previous work we also recommended that the Coast Guard evaluate its compliance inspection efforts taken during the initial 6-month period after July 1, 2004, and use the results as a means to strengthen its long-term strategy for ensuring compliance.[20] While the Coast Guard agreed with this recommendation, and has taken some steps to evaluate its compliance efforts, it has not conducted a comprehensive evaluation of these efforts to date. Without knowledge that the current approach to MTSA facility oversight is effective, the Coast Guard will be further challenged in planning future oversight activities.

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

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

[20]Ibid.

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

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

We have reported several times on the status of this program and the challenges that it faces.[21] Most recently, we reported that TSA has made progress in implementing the TWIC program and addressing problems we previously identified regarding contract planning and oversight and coordination with stakeholders.[22] For example, TSA reported that it added staff with program and contract management expertise to help oversee the contract and developed plans for conducting public outreach and education efforts.

The SAFE Port Act contained a requirement for implementing the first major phase of the TWIC program by mid-2007. More specifically, it required TSA to implement TWIC at the 10 highest risk ports by July 1, 2007, conduct a pilot program to test TWIC access control technologies in the maritime environment, issue regulations requiring TWIC card readers based on the findings of the pilot, and periodically report to Congress on the status of the program. TSA is taking steps to address these requirements, such as establishing a rollout schedule for enrolling workers

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

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

and issuing TWIC cards at ports and conducting a pilot program to test TWIC access control technologies.

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

- **Monitoring the effectiveness of contract planning and oversight.** While the steps that TSA reports taking are designed to address the contract planning and oversight problems that we have previously identified and recommendations we have made, the effectiveness of these steps will not be clear until implementation of the TWIC program begins.

- **Ensuring a successful enrollment process.** Significant challenges remain in enrolling about 770,000 persons at about 3,500 facilities in the TWIC program. Sufficient communication and coordination to ensure that all individuals and organizations affected by the TWIC program are aware of their responsibilities will require concerted effort on the part of TSA and the enrollment contractor.

- **Addressing access control technologies.** TSA and industry stakeholders need to address challenges regarding TWIC access control technologies to ensure that the program is implemented effectively. Without fully testing all aspects of the technology TSA may not be able ensure that the TWIC access control technology can meet the requirements of the system. Given the differences among the facilities and locations where the technology is to be implemented, it may be difficult to test all scenarios.

Multiple Background Check Programs for Transportation Workers Need to Be Coordinated

Since the terrorist attacks on September 11, 2001, the federal government has taken steps to ensure that transportation workers, many of whom transport hazardous materials or have access to secure areas in locations such as ports, are properly screened to ensure they do not pose a security risk. For example, the USA PATRIOT Act in October 2001 prohibited states from issuing hazardous material endorsements for a commercial driver's license without an applicant background check.[23] Background checks are also part of the TWIC program discussed above. Concerns have

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

been raised, however, that transportation workers may face a variety of background checks, each with different standards. A truck driver, for example, is subject to background checks for all of the following: unescorted access to a secure area at a port, unescorted access to a secure area at an airport, expedited border crossings, hauling hazardous materials, or hauling arms or ammunition for the Department of Defense or cargo for the U.S. Postal Service. In July 2004, the 9/11 Commission reported that having too many different biometric standards, travel facilitation systems, credentialing systems, and screening requirements hampers the development of information crucial for stopping terrorists from entering the country, is expensive, and is inefficient.[24] The Commission recommended that a coordinating body raise standards, facilitate information-sharing, and survey systems for potential problems. In August 2004, Homeland Security Directive 11 announced a new U.S. policy to "implement a coordinated and comprehensive approach to terrorist-related screening-in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure—that supports homeland security, at home and abroad."

DHS has taken steps, both at the department level and within its various agencies, to consolidate, coordinate, and harmonize such background check programs.[25] At the department level, DHS created the Screening Coordination Office (SCO) in July 2006 to coordinate DHS background check programs. The SCO is in the early stages of developing its plans for this coordination. In December 2006, SCO issued a report identifying common problems, challenges, and needed improvements in the credentialing programs and processes across the department. The office awarded a contract in April 2007 that will provide the methodology and support for developing an implementation plan to include common design and comparability standards and related milestones to coordinate DHS screening and credentialing programs. DHS components are currently in the initial stages of a number of their own initiatives. For example, In January 2007, TSA determined that the background checks required for three other DHS programs satisfied the background check requirement for

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

[25]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.

the TWIC program.[26] An applicant who has already undergone a background check in association with any of these three programs does not have to undergo an additional background check and pays a reduced fee to obtain a TWIC card. Similarly, the Coast Guard plans to consolidate four credentials and require that all pertinent information previously submitted by an applicant at a Coast Guard Regional Examination Center be submitted to TSA through the TWIC enrollment process.

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

- **Ensuring its plans are sufficiently complete without being overly restrictive.** The varied background check programs related to transportation workers may have substantially different standards or requirements. SCO will be challenged to coordinate DHS's background check programs in such a way that any common set of standards developed to eliminate redundant checks meets the varied needs of all the programs without being so strict that it unduly limits the applicant pool or so intrusive that potential applicants are unwilling to take part.

- **Ensuring that accurate performance information is available.** Without knowing the potential costs and benefits associated with the number of redundant background checks that would be eliminated through harmonization, DHS lacks the performance information that would allow its program managers to compare their program results with goals. Thus, DHS faces challenges in determining where to target program resources to improve performance. DHS could benefit from a plan that includes, at a minimum, a discussion of the potential costs and benefits associated with the number of redundant background checks that would be eliminated through harmonization.

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

- **Coordinating across the broader universe of federal background check programs.** Many other federal agencies also have background check programs, making coordination a cross-cutting, government-wide issue. DHS could face challenges harmonizing background check programs within DHS and other federal agencies.

Container Security Programs Maturing, but Implementation Challenges Continue

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

Automated Targeting System Continues to Require Management Action

As part of its responsibility for preventing terrorists and weapons of mass destruction from entering the United States, CBP addresses potential threats posed by the movement of oceangoing containers. CBP inspectors at seaports help determine which containers entering the country will undergo inspections and then perform physical inspections of such containers. To carry out this responsibility, CBP uses a layered security strategy that attempts to focus resources on potentially risky cargo containers while allowing other cargo containers to proceed without disrupting commerce. The ATS is one key element of this strategy. CBP uses ATS to review documentation, including electronic manifest information submitted by the ocean carriers on all arriving shipments, to help identify containers for additional inspection.[27] CBP requires the carriers to submit manifest information 24 hours prior to a United States-bound sea container being loaded onto a vessel in a foreign port. ATS is a complex mathematical model that uses weighted rules that assign a risk score to each arriving shipment based on manifest information. CBP inspectors use these scores to help them make decisions on the extent of documentary review or physical inspection to conduct.

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

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

The SAFE Port Act required that the CBP Commissioner take actions to improve ATS. These requirements included such steps as (1) having an independent panel review the effectiveness and capabilities of the ATS, (2) considering future iterations of ATS that would incorporate smart features, (3) ensuring that ATS has the capability to electronically compare manifest and other available data to detect any significant anomalies and facilitate their resolution, (4) ensuring that ATS has the capability to electronically identify, compile, and compare select data elements following a maritime transportation security incident, and (5) developing a schedule to address recommendations made by GAO and the Inspector General of the Department of the Treasury and DHS. Based on our findings and the further changes to the program enacted by the SAFE Port Act, we found the following challenge faced by CBP:

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

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

The CSI Program Has Matured but Challenges Remain

In response to the threat that a cargo container could be used to smuggle a weapon of mass destruction (WMD) into the United States, the U.S. Customs Service (now CBP) initiated the CSI in January 2002 to detect and deter terrorists from smuggling WMDs via containers before they reach domestic seaports. Under this initiative, foreign governments allow CBP personnel to be stationed at foreign seaports to identify container shipments at risk of containing WMD. CBP personnel refer high-risk shipments to host government officials, who determine whether to inspect the shipment before it leaves for the United States. Host government officials examine shipments with nonintrusive inspection equipment and, if they deem it necessary, open the cargo containers to physically examine the contents inside.[29] Since our last report on the CSI program, CBP has increased the number of seaports that participate in the program from 34 to 50, with plans to expand to a total of 58 ports by the end of this fiscal year.[30]

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

The SAFE Port Act formalized CSI into law and specified factors to be considered in designating seaports as CSI, including risk level, cargo volume, results of Coast Guard assessments, and the commitment of the host government to sharing critical information with DHS. The act also called for DHS to establish minimum technical criteria for the use of nonintrusive inspection equipment in conjunction with CSI and to require

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

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

that seaports receiving CSI designation operate such equipment in accordance with these criteria. Another provision related to container cargo requires DHS to ensure that integrated scanning systems, using nonintrusive imaging equipment and radiation detection equipment, are fully deployed to scan all containers before their arrival in the United States as soon as possible, but not before DHS determines that such systems meet a number of criteria. The SAFE Port Act addresses a number of the issues we have previously identified, but our work suggests that CBP may face continued challenges going forward. These challenges include:

- **Ensuring sufficient staff are available for targeting.** Although CBP's goal is to target all U.S. bound containers at CSI seaports before they depart for the United States, we previously reported that it has not been able to place enough staff at some CSI ports to do so.[31] Since then, CBP has provided additional support to deployed CSI staff by using staff in the United States (at the National Targeting Center) to screen containers for various risk factors and potential inspection.

- **Developing an international consensus on technical requirements.** There are no internationally recognized minimum technical requirements for the detection capability of nonintrusive inspection equipment used to scan containers. Consequently, host nations at CSI seaports use various types of nonintrusive inspection equipment and the detection capabilities of such equipment can vary. Because the inspection a container receives at a CSI seaport could be its only scan before entering the United States, it is important that the detection equipment used meets minimum technical requirements to provide some level of assurance that the presence of WMDs can be detected.

- **Ensuring that designated high-risk containers are inspected.** We also found that some containers designated as high risk did not receive an inspection at the CSI seaport. Containers designated as high risk by CSI teams that are not inspected overseas (for a variety of reasons) are supposed to be referred for inspection upon arrival at the U.S. destination port. However, CBP officials noted that between July and September 2004, only about 93 percent of shipments referred for domestic inspection were inspected at a U.S. seaport. According to

[31] GAO-05-557.

CBP, it is working on improvements in its ability to track such containers to assure that they are inspected.

DOE Has Made Progress with Megaports Program

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

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

When we reported on this program in March 2005, DOE had made limited progress in gaining agreements to install radiation detection equipment at the highest priority seaports.[32] At that time, DOE had completed work at only two ports and signed agreements to initiate work at five other ports. We also noted that DOE's cost projections for the program were uncertain, in part because they were based on DOE's $15 million estimate for the average cost per port. This per port cost estimate may not be accurate

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

because it was based primarily on DOE's radiation detection assistance work at Russian land borders, airports, and seaports and did not account for the fact that the costs of installing equipment at individual ports vary and are influenced by factors such as a port's size, its physical layout, and existing infrastructure. Since our review, DOE has developed a strategic plan for the Megaports Initiative and is in the process of revising its per port cost estimate.

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

- **Ensuring the ability to detect radioactive material.** Certain factors can affect the general capability of radiation detection equipment to detect nuclear material. For example, some nuclear materials can be shielded with lead or other dense materials to prevent radiation from being detected. In addition, one of the materials of greatest proliferation concern, highly enriched uranium, is difficult to detect because of its relatively low level of radioactivity.

- **Overcoming the physical layout of ports.** In its effort to screen cargo containers at foreign ports for radioactive and nuclear materials, DOE faces technical challenges related to these ports' physical layouts and cargo stacking configurations. To address a part of these challenges at some ports, DOE is testing at Freeport, Bahamas, a device used to transport cargo containers between port locations—known as a straddle carrier—that is outfitted with radiation detection equipment.

- **Sustaining equipment in port environments.** Additionally, environmental conditions specific to ports, such as the existence of high winds and sea spray, can affect the radiation detection equipment's performance and long-term sustainability. To minimize the effects of these conditions, DOE has used steel plates to stabilize radiation portal monitors placed in areas with high winds, such as in Rotterdam, and is currently evaluating approaches to combat the corrosive effects of sea spray on radiation detection equipment.

Secure Freight Initiative Only Recently Announced

In another provision related to container security and the work to address WMD and related risks, the SAFE Port Act specified that new integrated scanning systems that couple nonintrusive imaging equipment and radiation detection equipment must be pilot tested at three international

seaports. It also required that, once fully implemented, the pilot integrated scanning system scan 100 percent of containers destined for the United States that are loaded at such ports. To fulfill these requirements, DHS and DOE jointly announced the formation of a pilot program called the Secure Freight Initiative (SFI) in December 2006, as an effort to build upon existing port security measures by enhancing the U.S. government's ability to scan containers for nuclear and radiological materials overseas and better assess the risk of inbound containers. In essence, SFI builds upon the CSI and Megaports programs.

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

We have not yet reviewed the efforts made under SFI. However, in carrying it out, the agencies may likely have to deal with the challenges previously identified for the CSI and Megaports programs. Per the SAFE Port Act, DHS is to report by April 2008 on, among other things, the lessons learned from the SFI pilot ports and the need for and the feasibility of expanding the system to other CSI ports, and every 6 months thereafter, DHS is to report on the status of full-scale deployment of the integrated scanning systems to scan all containers bound for the United States before their arrival.

C-TPAT Maturing, but Validation and Other Management Challenges Remain

C-TPAT, initiated in November 2001, is designed to complement other container security programs as part of a layered security strategy. C-TPAT is a voluntary program that enables CBP officials to work in partnership with private companies to review the security of their international supply chains and improve the security of their shipments to the United States. In return for committing to improving the security of their shipments by joining the program, C-TPAT members receive benefits that result in reduced scrutiny of their shipments, such as a reduced number of inspections or shorter wait times for their shipments. Since C-TPAT's inception, CBP has certified 6,375 companies, and as of March 2007, it had validated the security of 3,950 of them (61.9 percent).

CBP initially set a goal of validating all companies within their first 3 years as C-TPAT members, but the program's rapid growth in membership made the goal unachievable. CBP then moved to a risk-based approach to selecting members for validation, considering factors such as the company having foreign supply chain operations in a known terrorist area or involving multiple foreign suppliers. CBP further modified its approach to selecting companies for validation to achieve greater efficiency by conducting "blitz" operations to validate foreign elements of multiple members' supply chains in a single trip. Blitz operations focus on factors such as C-TPAT members within a certain industry, supply chains within a certain geographic area or foreign suppliers to multiple C-TPAT members. Risks remain a consideration, according to CBP, but the blitz strategy drives the decision of when a member company will be validated.

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

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

The SAFE Port Act formalized C-TPAT into law. In addition, it included a new goal that CBP validate C-TPAT members' security measures and supply chain security practices within 1 year of their certification and revalidate those members no less than once in every 4 years. CBP faces several challenges in addressing this requirement and dealing with the concerns we previously identified. These challenges include:

- **Conducting validations within 1 year.** The goal of completing validations within a year of members' certification is a challenge. While CBP has belatedly reached some of its earlier staffing goals, consistent membership growth has led to a steady backlog of validation requirements.

- **Ensuring sound validations.** CBP's standard for validations—to ensure that members' security measures are reliable, accurate and effective—is hard to achieve. Since C-TPAT is a voluntary rather than a mandatory program, there are limits on how intrusive CBP can be in its validations. Further, CBP lacks jurisdiction over foreign companies operating outside the United States in a member's foreign supply chain; therefore its ability to review the complete supply chain of a member is questionable.

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

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

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

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

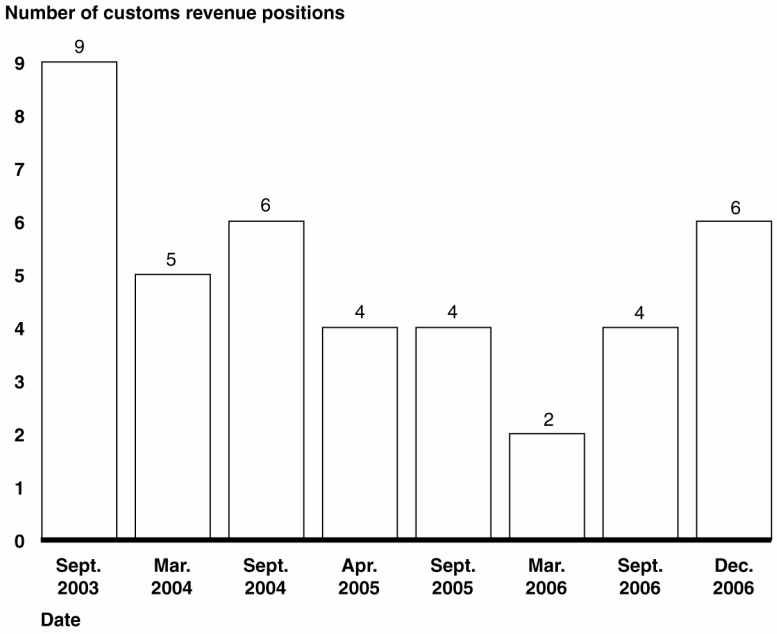
Staff resources contributing to customs revenue functions generally declined since the formation of DHS in March 2003, in part due to department priorities focused on homeland security and recruiting and retention problems for some positions. As shown in figure 1, since September 2003, CBP has not maintained the mandated number of staff in each of the nine designated customs revenue positions, although recent efforts by CBP increased the number of staff to the mandated levels in most of these positions as of December 2006. For example, the number of Import Specialists on board dropped from 984 in March 2003 to a low of 892 in March 2006, and grew to 1,000 in December 2006. CBP was below

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

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

the mandated staff levels for three customs revenue positions as of December 2006, ranging from 2 to 34 positions below the baseline. Recently, CBP took several steps such as opening job announcements and closely monitoring its customs revenue staffing levels to increase the number of customs revenue staff by more than 130 to 2,273.[36]

Figure 1: Number of Customs Revenue Positions for Which CBP Maintained the Mandated Staffing Levels

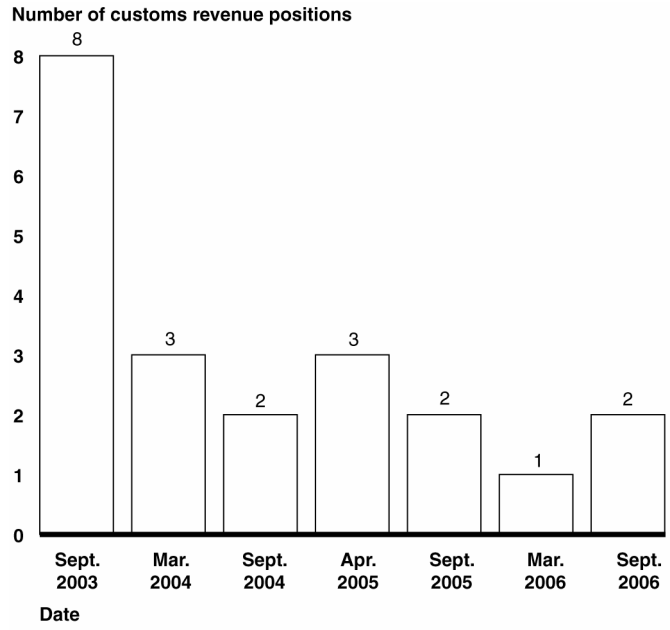


Source: GAO analysis of CBP data.

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

[36] See appendix I for more information on staff levels over time.

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



Source: GAO analysis of CBP data.

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

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

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

Additionally, external and internal challenges heighten the importance of such strategic workforce planning. First, the workload for some customs revenue positions has increased. For example, the growing number of free trade agreements has had a pronounced effect on some customs revenue positions, including attorneys in CBP's Office of Regulations and Rulings who participate in every phase of the negotiation and implementation of the free trade agreements—from participating in negotiating sessions through issuing binding rulings regarding the proper interpretation of the CBP regulations implementing the agreement. In addition, some customs revenue positions have seen an expansion of revenue-related as well as nonrevenue-related responsibilities. For instance, with the formation of DHS, the Fines, Penalties, and Forfeitures Specialists from the former Customs Service became responsible for administering fines and penalties for violations of immigration and agriculture laws in addition to their existing responsibilities related to customs law. Also, staff in some customs revenue positions told us they have been assigned work that is unrelated to customs revenue functions. For example, one port has not had a Secretary/Receptionist position for 5 years. As a result, that function was given to Import Specialists on a rotational basis.

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

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

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

Concluding Observations

MTSA established a maritime security framework that the Coast Guard implemented with area maritime security committees, area maritime security plans, and exercises to test the plans. In addition, various agencies showed initiative in establishing other programs related to maritime security—such as the Coast Guard, DOD and DOJ establishing interagency operations centers; CBP implementing CSI and C-TPAT; and DOE establishing the Megaports Inititive. In some cases, agencies have struggled to implement programs required by MTSA or other legislation—

such as TSA delays with the TWIC program and CBP not meeting required staffing levels for customs revenue functions. The SAFE Port Act further defined and strengthened this maritime security framework—and created additional requirements for agencies at a time when their programs are still maturing. We have reviewed many of the MTSA and SAFE Port Act related programs and made recommendations to develop strategic plans, better plan their use of human capital, establish performance measures, and otherwise improve the operations of these programs. In general, these agencies have concurred with our recommendations and are making progress implementing them. We will continue to monitor these programs and provide Congress with oversight and insight into maritime security.

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

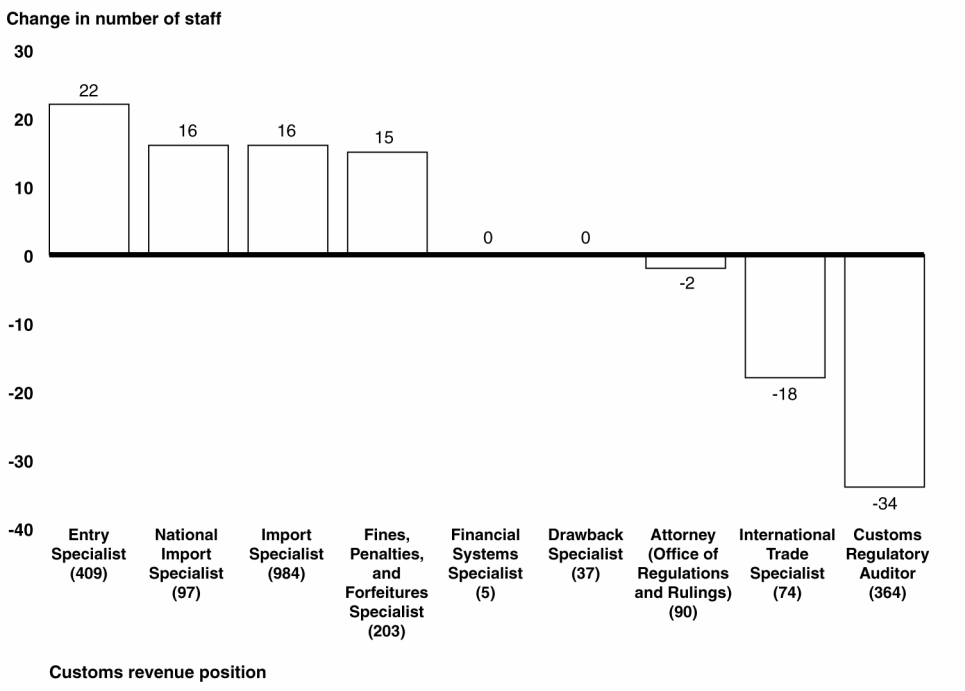
GAO Contact and Staff Acknowledgements

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 Jonathan Bachman, Jason Bair, Fredrick Berry, Christine Broderick, Stockton Butler, Steven Calvo, Christopher Currie, Wayne Ekblad, Christopher Hatscher, Monica Kelly, Tracey King, Daniel Klabunde, Gary Malavenda, Robert Rivas, and Stan Stenersen.

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

This appendix provides information on the number of staff in specific customs revenue functions positions from the creation of the Department of Homeland Security (DHS) until late in 2006. The change in the number of staff in customs revenue positions and their associated support staff varies by position. Figure 3 shows the change in the number of staff in customs revenue positions; figure 4 shows the change in the number of associated support staff.

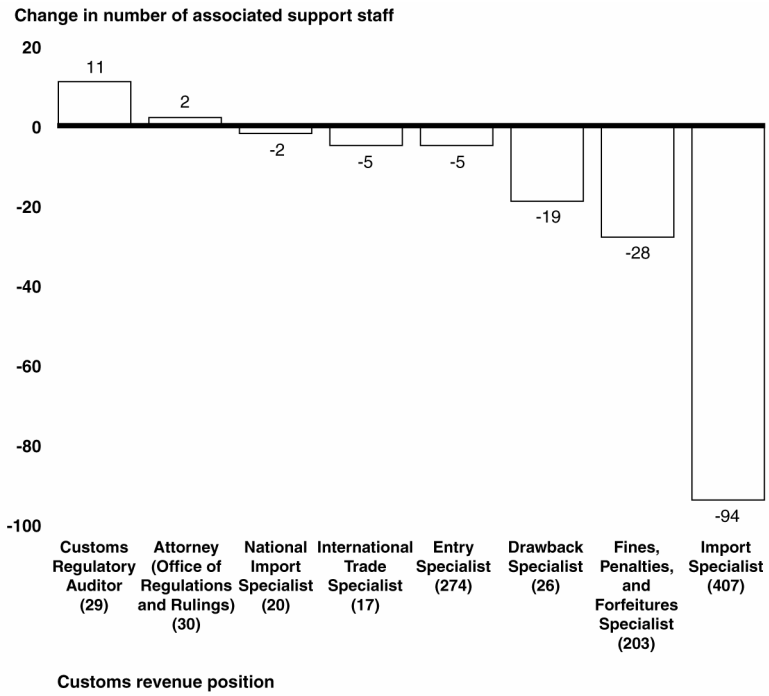
Figure 3: Change in Number of Staff in Customs Revenue Positions from March 2003 Baseline, as of December 2006



Source: GAO analysis of CBP data.

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

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



Source: GAO analysis of CBP data.

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

Related GAO Products:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 "Subscribe to 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, D.C. 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, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548