United States Government Accountability Office

GAO

Testimony

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

For Release on Delivery
Expected at 10 a.m. EDT
Tuesday, May 17, 2005

MARITIME SECURITY

Enhancements Made, But Implementation and Sustainability Remain Key Challenges

Statement of Margaret T. Wrightson
Director, Homeland Security and Justice Issues

GAO
Accountability * Integrity * Reliability

Highlights of GAO-05-448T, a testimony before the Committee on Commerce, Science, and Transportation, United States Senate

May 17, 2005

MARITIME SECURITY

Enhancements Made, But Implementation and Sustainability Remain Key Challenges

Why GAO Did This Study

More than 3 years after the terrorist attacks of September 11, 2001, concerns remain over the security of U.S. seaports and waterways. Seaports and waterways are vulnerable given their size, easy accessibility by water and land, large numbers of potential targets, and close proximity to urban areas. Seaports are also a critical link in the international supply chain, which has its own potential vulnerabilities that terrorists could exploit to transport a weapon of mass destruction to the United States. Federal agencies such as the Coast Guard and Customs and Border Protection and other seaport stakeholders such as state and local law enforcement officials as well as owners and operators of facilities and vessels have taken actions to try to mitigate these vulnerabilities and enhance maritime security.

This testimony, which is based on previously completed GAO work, reports on (1) the types of actions taken by the federal government and other stakeholders to address maritime security, (2) the main challenges that GAO observed in taking these actions, and (3) what tools and approaches may be useful in planning future actions to enhance maritime security.

What GAO Recommends

This testimony makes no recommendations but cites several reports in which recommendations were previously made.

www.gao.gov/cgi-bin/getrpt?GAO-05-448T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Margaret Wrightson at (415) 904-2200 or WrightsonM@gao.gov.

What GAO Found

Federal agencies and local stakeholders have taken many actions to secure seaports. For example, federal agencies have stepped up vessel monitoring, cargo and container inspection, and security patrol activities. Port stakeholders in the private sector and in state and local government have taken such actions as conducting security assessments of infrastructure and vessels and implementing security plans. These actions provide three types of protections: identifying and reducing vulnerabilities of seaports, securing the cargo moving through seaports, and developing an informed view of maritime activities through intelligence, information-sharing, and new technologies to identify and respond to threats.

Due in large part to the urgency with which these actions were implemented, challenges have been encountered in implementing them. While some challenges may be resolved with time, others are more difficult to resolve and could hinder the actions' effectiveness. The main challenges GAO has identified include failure to develop necessary planning components to carry out the programs; difficulty in coordinating the activities of federal agencies and port stakeholders to implement programs; and difficulty in maintaining the financial support to continue implementation of security enhancements.

As intensified homeland security efforts continue, assessing their contribution to security and their sustainability over time will become more important. Assessing the progress made in securing seaports is difficult, as these efforts lack clear goals defining what they are to achieve and measures that track progress toward these goals. As Congress and the nation consider how much security is enough, more attention will likely be needed to define these goals and measures. Doing so is important because no amount of money can totally protect seaports from attack by a determined enemy. These realities suggest that the future focus in applying resources and efforts needs to incorporate an approach to assess critical infrastructure, determine what is most at risk, and apply measures designed to make cost effective use of resources and funding.

Seaports are difficult to secure due to their size, ease of accessibility by water and land, variety of potential targets, and close proximity to urban areas.

Source: Port of Los Angeles.

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss the nation's efforts to improve seaport security. More than 3 years after the terrorist attacks of September 11, 2001, seaport security continues to be a major concern for the nation. For example, many seaport areas are inherently vulnerable, given their size, easy accessibility by water and land, large numbers of potential targets, and proximity to urban areas. Also, the large cargo volumes passing through seaports, such as containers destined for further shipment by other modes of transportation such as rail or truck, also represent a potential conduit for terrorists to smuggle weapons of mass destruction or other dangerous materials into the United States. The potential consequences of the risks created by these vulnerabilities are significant as the nation's economy relies on an expeditious flow of goods through seaports. A successful attack on a seaport could result in a dramatic slowdown in the supply system, with consequences in the billions of dollars.

Much has been set in motion to address these risks in the wake of the September 11, 2001, terrorist attacks. Both Congress and the administration have been active, through legislation, presidential directives, and international agreements, in enhancing seaport security. Key agencies, such as the Coast Guard, the Customs Service, and the Transportation Security Administration (TSA), have been reorganized under the new Department of Homeland Security (DHS) and tasked with numerous responsibilities designed to strengthen seaport security. Many of these tasks were required by the Maritime Transportation Security Act of 2002 (MTSA).[1]

My testimony today draws primarily on the work we have done in responding to congressional requests for information and analysis about the nation's homeland security efforts (see app. I for a list of recent reports and testimonies we have issued). We conducted 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. Over the course of completing this work, we have made a number of recommendations for specific agencies, which can be found in appendix II. While this body of work does not cover every program or action that has been taken, it does encompass a wide range of these

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

actions. My testimony will (1) provide an overview of the types of actions taken by the federal government and other stakeholders to address seaport security, (2) describe the main challenges encountered in taking these actions, and (3) describe what tools and approaches may be useful in charting a course for future actions to enhance security.

In summary:

Seaports are vulnerable on many fronts and the actions taken to secure them can be divided into three main categories: reducing vulnerabilities of specific targets within seaports, making the cargo flowing through these seaport gateways more secure, and developing what is called "maritime domain awareness"—a sufficiently informed view of maritime activities by stakeholders involved in security to quickly identify and respond to emergencies, unusual patterns or events, and matters of particular interest. Within each category, several actions have been taken or are underway. For example, assessments of potential targets have been completed at 55 of the nation's most economically and militarily strategic seaports, and more than 9,000 vessels and over 3,000 facilities have developed security plans and have been reviewed by the Coast Guard. Customs inspectors have been placed at some overseas seaports and partnerships struck up with some private sector stakeholders to help ensure that the cargo and containers arriving at U.S. seaports are free of weapons of mass destruction (WMD) or a radiological "dirty bomb." New assets are budgeted and are coming on line, including new Coast Guard boats and cutters and communication systems. Finally, new information-sharing networks and command structures have been created to allow more coordinated responses and increase awareness of activities going on in the maritime domain. Some of these efforts have been completed and others are ongoing; overall, the amount of effort has been considerable.

The efforts we have reviewed over the past 3 years, many of which were quickly implemented to address pressing security needs, have encountered challenges that could significantly affect their success. Some of these challenges are likely to be resolved with time, but some reflect greater difficulty and therefore merit more attention. The more complex challenges take three main forms:

- Program design and implementation: Some agencies have failed to design programs and planning components, such as human capital plans and performance measures, that are necessary to successfully implement their programs and ensure they are effective. For example, U.S. Customs and Border Protection (CBP) started implementation of two key container supply chain security initiatives before taking adequate steps to develop plans and strategies to effectively manage critical aspects of the programs such as human capital and achievement of program objectives.

- Coordinating security efforts with stakeholders: Many private sector companies and governmental agencies are involved in seaport security efforts, and in some cases progress has been hampered because of difficulties in communication and coordination between parties. For example, deadlines in the development of an identification card for transportation workers have been missed due in part to a lack of communication and coordination between TSA and DHS.

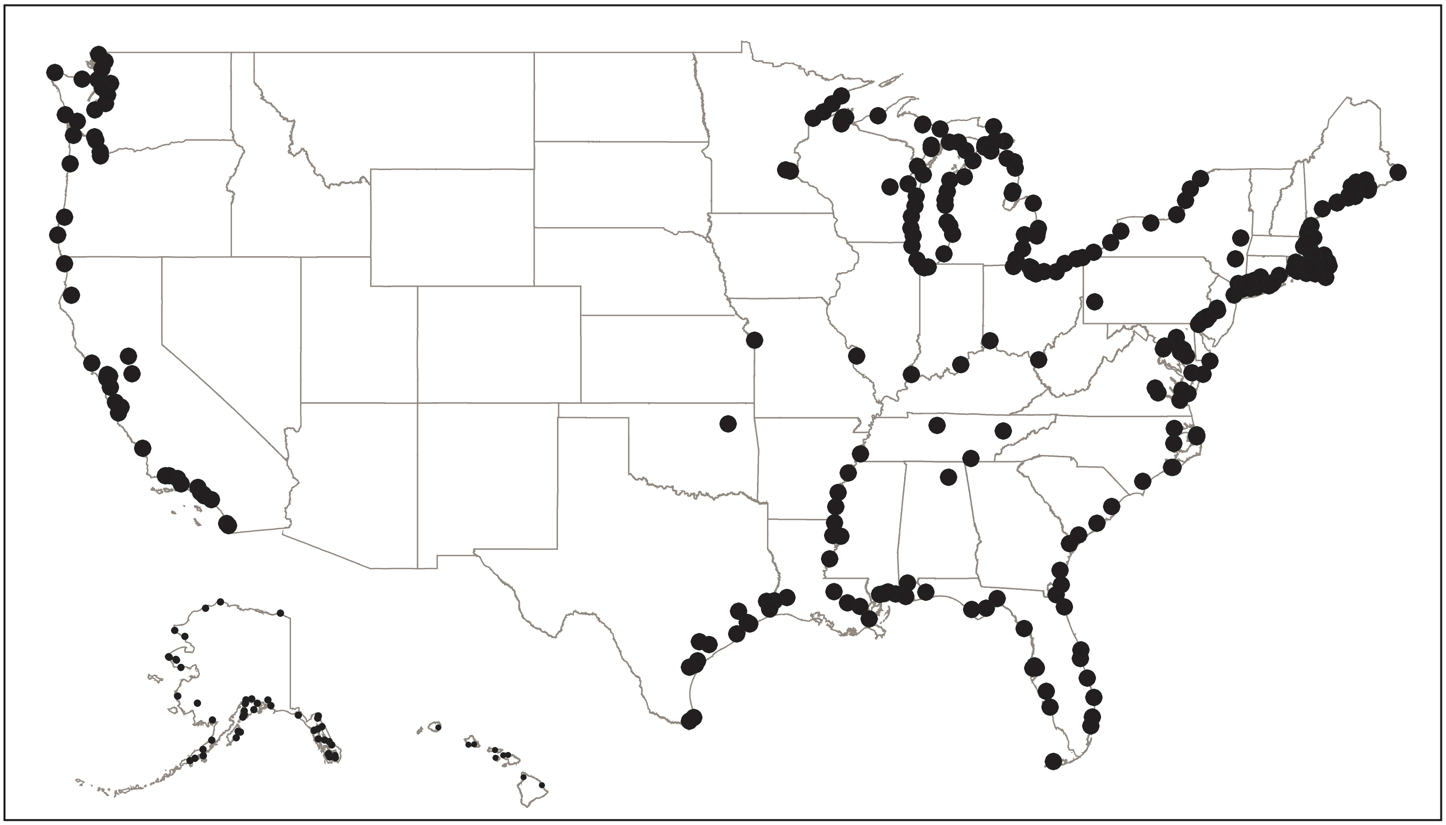
- Funding security improvements: Economic constraints, such as declining revenues and increased security costs, make it difficult to provide and sustain the funding necessary to continue implementing security measures and activities by maritime stakeholders including the federal government. Consequently, many stakeholders rely heavily on the federal government for assistance, and requests for federal grant funding far outstrip the funding amounts available. For example, although more than $560 million in grants has been awarded to seaport stakeholders since 2002 under federal grant programs for implementation of security measures and activities, this amount has met only a fraction of the amount requested by these stakeholders.

As actions to enhance homeland security continue, and as it becomes clearer that the price of these actions will be measured in the billions of dollars, it is likely that increasing attention will turn to assessing the progress made in securing seaports and determine where future actions and funds should be allocated to further enhance security. Although there is widespread agreement that actions taken so far have led to a heightened awareness of the need for security and an enhanced ability to identify and respond to many security threats, assessing the degree of progress in making the nation more secure is difficult. Thus far, seaport security actions—and homeland security activities in general—lack performance measures to define what these activities are intended to achieve and measure progress toward these goals. As Congress and the nation continue to evaluate how much security is enough, more attention on defining these goals and measures will likely be needed by stakeholders. Doing so is all the more important because, as groups such as the 9/11 Commission have pointed out, no amount of money can totally insulate seaports from attack by a well-funded and determined enemy. These realities suggest that the future focus in applying resources and efforts also needs to incorporate an approach to identify and manage risk—that is, on assessing critical infrastructure, determining what is most at risk, and applying sound measures designed to make cost-effective use of resources and funding.

Background

The vast U.S. maritime system contains more than 300 seaports and 3,700 cargo and passenger terminals. These seaports dot not only our seacoasts, but also major lakes and rivers (see fig. 1). Much of the nation's commercial maritime activities, however, are concentrated in about a dozen major seaports, such as Los Angeles-Long Beach, New York-New Jersey, and Houston.

Figure 1: Location of U.S. Seaports



Source: GAO presentation of TSA, Department of Transportation's Bureau of Transportation statistics, and Federal Transit Administration data.

The nation's seaports are economic engines and a key part of the national defense system. More than 95 percent of the nation's non-North American foreign trade (and 100 percent of certain commodities, such as foreign oil) arrives by ship. Cargo containers, approximately 7 million of which entered the country in 2002, are central to an efficient transportation network because they can be quickly shifted from ships to trains and trucks and back again. Because of these efficiencies, the U.S. and world economies have become increasingly reliant on cargo containers to transport their goods. With regard to national security, the Departments of Defense and Transportation have designated 17 U.S. seaports as strategic because they are necessary for use in the event of a major military deployment. Thirteen of them are commercial seaports.

While the terrorist attacks of September 11, 2001, did not involve seaports, they called attention to ways in which seaports represent an attractive and vulnerable terrorist target. Various studies have pointed out that significant disruptions could result from a seaport-related attack. For example, the Brookings Institution has estimated that costs associated with U.S. seaport closures resulting from a detonated weapon of mass destruction could amount to $1 trillion. The firm of Booz, Allen, and Hamilton studied the potential cost of discovering an undetonated weapon of mass destruction at a U.S. seaport and placed the cost of a 12-day closure of seaports at approximately $58 billion. An actual closure of seaports along the West Coast occurred for 10 days in 2002 due to a labor dispute. According to one estimate, the cost of this closure to the national economy for the first 5 days was estimated at $4.7 billion and increased exponentially after that.[2] Similarly, if 1 or more of the 17 strategic U.S. seaports (or the ships carrying military supplies) were successfully attacked, not only could massive civilian casualties be sustained and critical infrastructure lost, but the military could also lose precious cargo and time and be forced to rely heavily on already burdened airlift capabilities.

Many Actions Have Been Taken or Are Underway to Address Seaport Security

Since September 11, 2001, a number of actions have been taken or are underway to address seaport security by a diverse mix of agencies and seaport stakeholders. Federal agencies, such as the Coast Guard, U.S. Customs and Border Protection (CBP), and TSA, have been tasked with responsibilities and functions intended to make seaports more secure, such as monitoring vessel traffic or inspecting cargo and containers, and

[2] Zeigert, Amy, et. al. “Port Security: Improving Emergency Response Capabilities at the Ports of Los Angeles and Long Beach.” *California Policy Options 2005.* University of California Los Angeles, School of Public Affairs (Los Angeles, Calif. 2005).

procuring new assets such as aircraft and cutters to conduct patrols and respond to threats. In addition to these federal agencies, seaport stakeholders in the private sector and at the state and local levels of government have taken actions to enhance the security of seaports, such as conducting security assessments of infrastructure and vessels operated within the seaports and developing security plans to protect against a terrorist attack. The actions taken by these agencies and stakeholders are primarily aimed at three types of protections: (1) identifying and reducing vulnerabilities of the facilities, infrastructure, and vessels operating in seaports, (2) securing the cargo and commerce flowing through seaports, and (3) developing greater maritime domain awareness through enhanced intelligence, information-sharing capabilities, and assets and technologies.

Identifying and Reducing the Vulnerabilities of Facilities, Infrastructure, and Vessels

Seaports facilitate the freedom of movement and flow of goods, and in doing so they allow people, cargo, and vessels to transit with relative anonymity. While seaports contain terminals and other facilities where goods bound for import or export are unloaded and loaded, or where people board and disembark cruise ships or ferries, seaports also often contain other infrastructure critical to the nation's economy and defense, such as military installations, chemical factories, powerplants, and refineries. The combination of assets, access, and anonymity makes for potentially attractive targets. The facilities and vessels in seaports can be vulnerable on many fronts. For example, facilities where containers are transferred between ships and railroad cars or trucks must be able to screen vehicles entering the facility and routinely check cargo for evidence of tampering. Chemical factories and other installations where hazardous materials are present must be able to control access to areas containing dangerous goods or hazardous substances. Vessels, ranging from oil tankers and freighters to tugboats and passenger ferries, must be able to restrict access to certain areas on board the vessel, such as the bridge or other control stations critical to the vessel's operation.

Given the wide range of potential targets, an effective security response includes identifying targets, assessing risks to them, and taking steps to reduce or mitigate these risks. An essential step in this process is to conduct a security or vulnerability assessment. This assessment, which is needed both for the seaport as a whole and for individual vessels and facilities, identifies vulnerabilities in physical structures, personnel protection systems, processes, and other areas that may lead to a security breach. For example, this assessment might reveal weaknesses in an organization's security systems or unprotected access points such as a facility's perimeter not being sufficiently lighted or gates not being secured or monitored after hours. After the vulnerabilities are identified, measures can be then be identified that will reduce or mitigate the vulnerabilities when installed or implemented.

Most actions to identify and reduce the vulnerabilities within seaports were specifically required by the Maritime Transportation Security Act of 2002 (MTSA). Passage of MTSA was a major step in establishing a security framework for America's seaports. This security framework includes assessment of risks, access controls over personnel and facilities, and development and implementation of security plans, among other activities. Table 1 shows some of the actions that have been taken and programs that are in the process of being implemented to carry out this framework. [3]

[3] None of the listings in this testimony is meant to be exhaustive of all the efforts under way. The Coast Guard has a range of activities underway for reducing seaport vulnerabilities that extends beyond the actions shown here. Such activities include, among others the use of armed boarding officers, formerly known as sea marshals, who board high-interest vessels arriving or departing U.S. seaports and stand guard in critical areas of the vessels; the establishment of Maritime Safety and Security Teams (MSST) to provide antiterrorism protection for strategic shipping, high-interest vessels, and critical infrastructure; and the underwater port security system, which uses trained divers and robotic cameras to check ship hulls and piers and an underwater intruder detection system. We have not evaluated the effectiveness of these activities.

Table 1: Examples of Actions Taken and Programs Underway to Identify and Reduce Vulnerabilities

Action or program	Description
Conducting security assessments and developing security plans for facilities and vessels	MTSA and its implementing regulations require designated owners or operators of maritime facilities or vessels to identify vulnerabilities and develop security plans for their facilities or vessels. The plans were reviewed and approved by the Coast Guard. Since July 1, 2004, the Coast Guard has been conducting inspections of these facilities and vessels to ensure the plans have been implemented. The Coast Guard completed inspections of the facilities by December 31, 2004, and is scheduled to complete inspections of the vessels by July 1, 2005.
Conducting security assessments and developing seaport-wide security plans	To meet another MTSA requirement, the Coast Guard led efforts to conduct a seaport-wide security assessment of each of the nation's seaports and develop a security plan for the seaport zone. In carrying out these efforts, the Coast Guard worked with a wide variety of stakeholders, such as state and local governments, law enforcement, owners and operators of facilities and vessels, and trade and labor organizations.
Development of the Transportation Worker Identification Credential (TWIC)	TWIC is designed to respond to various statutory provisions relating to transportation related worker identification including MTSA, which requires a biometric identification card be issued to individuals requiring unescorted access to secure areas of seaport facilities or vessels. This credential is being designed to be a universally recognized identification card accepted across all modes of the national transportation system, including airports, railroad terminals, and seaports.
Port Security Assessment Program	Separate from MTSA requirements, the Coast Guard established a program after September 11, 2001, to assess vulnerabilities of the nation's 55 most strategic commercial and military seaports. The program has changed considerably since its inception and now includes a geographic information system (GIS) to help identify and provide up-to-date information on threats and incidents, as well as provide accessible information to help develop security plans.

Source: GAO analysis of Coast Guard and TSA data.

The amount of effort involved in carrying out these actions and implementing these programs has been considerable. For example, after following an aggressive time frame to develop regulations to implement the requirements of MTSA, the Coast Guard reviewed and approved the security plans of the over 3,000 facilities and more than 9,000 vessels that were required to identify their vulnerabilities and take action to reduce them. Six months after July 1, 2004, the date by which the security plans were to be implemented, the Coast Guard reported that it completed on-site inspections of all facilities and thousands of vessels to ensure the plans were being implemented as approved. In addition to its work on the security plans and inspections, the Coast Guard completed security assessments of the nation's 55 most economically and militarily strategic seaports.

Securing the Cargo Flowing through Seaports

While the facilities, vessels, and infrastructure within seaports have vulnerabilities to terrorist attack, the cargoes transiting through seaports also have vulnerabilities that terrorists could exploit. Containers are of particular concern because they can be filled overseas at so many different locations and are transported through complex logistics networks before reaching U.S. seaports. From the time the container is loaded for shipping to the time the container arrives at a seaport, the containers must go through several steps that involve many different participants and many points of transfer. Each of these steps in the supply chain presents its own vulnerabilities that terrorists could take advantage of to place a WMD into a container for shipment to the United States. A report prepared by the National Defense University's Center for Technology and National Security Policy stated that a container is ideally suited to deliver a WMD or a radiological "dirty bomb." While there have been no known incidents yet of containers being used to transport WMDs, criminals have exploited containers for other illegal purposes, such as smuggling weapons, people, and illicit substances. Such activities demonstrate the vulnerability of the freight transportation industry and suggest opportunities for further exploitation of containers by criminals, including terrorist groups.

In general, the actions taken thus far are aimed at identifying, tracking, and scrutinizing the container cargo shipments moving into the country. Most of these actions are being done by CBP, the DHS agency responsible for protecting the nation's borders and official ports of entry. CBP uses a layered approach that attempts to focus resources on potentially risky cargo containers while allowing other cargo containers to proceed without disrupting commerce. This approach includes the actions and programs shown in table 2. Several of these actions involve a strategy of moving primary reliance for security away from control systems at U.S. seaports of entry and toward improved controls at points of origin and along the way.[4]

[4] Another program to help secure the overseas supply chain process is the Coast Guard's International Port Security Program. In response to being required under MTSA to assess antiterrorism measures maintained at foreign seaports, the Coast Guard established this program in April 2004 to protect the global shipping industry by helping foreign nations evaluate security measures in their seaports. Through bilateral or multilateral discussions, the Coast Guard and the host nations review the implementation of security measures against established security standards, such as the International Maritime Organization's ISPS Code. To conduct the program, the Coast Guard has assigned officials to three regions (Asia-Pacific, Europe/Africa/Middle East, and Central/South America) to facilitate the discussions. In addition, a Coast Guard team has been established to conduct country/port visits, discuss security measures implemented, and develop best practices between countries. Each year the Coast Guard seeks to visit approximately 45 countries that conduct maritime trade with the United States.

Table 2: Examples of Container Security Actions

Action	Description
Automated Targeting System (ATS)	A computer model reviews documentation on all arriving containers and helps select or target containers for additional scrutiny.
Supply Chain Stratified Examination	Supplements ATS by randomly selecting additional containers to be physically examined. The results of the random inspection program are to be compared with the results of ATS inspections to improve targeting.
Container Security Initiative (CSI)	Places staff at designated foreign seaports to work with foreign counterparts to identify and inspect high-risk containers for weapons of mass destruction before they are shipped to the United States.
Customs-Trade Partnership Against Terrorism (C-TPAT)	Cooperative program between CBP and members of the international trade community in which private companies agree to improve the security of their supply chains in return for a reduced likelihood that their containers will be inspected.
Operation Safe Commerce	Begun by the private sector and now administered by DHS's Office of Domestic Preparedness, efforts center on (1) ensuring that containers are loaded in a secure environment at the point of product origin, with 100 percent verification of their contents; (2) using such technology as pressure, light, or temperature sensors to continually monitor containers throughout their overseas voyage to the point of distribution in the United States; and (3) using cargo-tracking technology to keep accurate track of containers at all points in the supply chain, including distribution to their ultimate destinations.
Megaports Initiative	In 2003, the Department of Energy (DOE) initiated the Initiative to enable foreign government personnel at key seaports to use radiation detection equipment to screen shipping containers entering and leaving these seaports for nuclear and other radioactive material that could be used against the United States or its allies. Through the Initiative, DOE installs radiation detection equipment at foreign seaports that is then operated by foreign government officials and port personnel working at these seaports.

Source: GAO analysis of CBP and DOE data.

The table also shows Operation Safe Commerce, initiated by the private sector and now administered by DHS's Office of Domestic Preparedness, which employs a similar strategy. This action, in pilot-project form that was initially funded by $58 million appropriated by Congress, is intended to help strengthen the security of cargo as it moves along the international supply chain in containers.[5] In late 2004, the second of two initial phases of the project was concluded. This phase involved identifying the security vulnerabilities of 19 separate supply chains and trying out technologies, such as container seals or sensors, and their integration with governmental policies, logistic processes and procedures that could mitigate those vulnerabilities. The project has received additional funding

[5] The nation's three largest container port regions (Los Angeles/Long Beach, New York/New Jersey, and Seattle/Tacoma) are involved in the Operation Safe Commerce pilot project.

of $17 million that has been targeted to conduct a third phase in which the best technologies and practices identified in the first two phases will be further tested on a high number of containers for their effectiveness and tamper resistance on three separate supply chains. A report on the best practices identified in the first two phases is expected to be issued in June 2005, and completion of the third phase is expected by October 2006.

The other actions taken to enhance the security of cargo and commerce have been substantial. In 2002 CBP quickly rolled out the CSI and C-TPAT programs shown in table 2 and enlisted the participation of several countries and companies. By April 2005, CSI was operational at 35 seaports, located in 18 countries. Similarly, C-TPAT membership grew from about 1,700 companies in January 2003 to over 9,000 companies in March 2005. Given the urgency to take steps to protect against terrorism after the September 11, 2001, attacks, some of the actions were taken using an “implement and amend” approach. That is, CBP had to immediately implement the activity with the knowledge it may need to modify the approach later. For example, in August 2002, CBP modified the already developed Automatic Targeting System with new terrorism-related criteria.

Developing Greater Maritime Domain Awareness

The third main area of activity to enhance seaport security—maritime domain awareness—is the understanding by stakeholders involved in maritime security of anything associated with the global maritime environment that could adversely affect the security, safety, economy or environment of the United States. This awareness is essential to identify and respond to any unusual patterns or anomalies that could portend a possible terrorist attack. To be effective, maritime domain awareness must be comprehensive and include information on vessels, seaport infrastructures and facilities, shipping lanes and transit corridors, waterways, and anchorages, among other things. It must also identify threats as soon as possible and far enough away from U.S. seaports to eliminate or mitigate the threat. By effectively identifying potential threats, this awareness can be used as a force multiplier to position resources where they are needed most to respond, instead of spreading out limited resources to address all threats, no matter how unlikely they are to occur. In addition, when shared, this awareness has the potential to facilitate the coordination of efforts of local, state, federal, and even international stakeholders in responding to potential threats.

After the attacks of September 11, 2001, the Coast Guard took steps such as increasing the number of security patrols conducted within seaports and waterways that helped contribute to increased maritime domain awareness. Although maritime homeland security duties are not new to the Coast Guard, the number of hours the Coast Guard used resources (such as ships, boats, or aircraft) to carry out seaport, waterway, and coastal security activities during fiscal year 2003 increased by 1,220 percent from their pre-September 11, 2001, level. Relative to the rest of the Coast Guard's responsibilities, this represented an increase from 4 percent of the Coast Guard's total annual resource hours being used for seaport, waterway, and coastal security activities before September 11, 2001, to 34 percent by September 30, 2003. These activities provide an important input to maritime domain awareness as it places Coast Guard personnel out in the seaports where they can observe, report, and respond to suspect activities or vessels. In addition, these patrols provide the Coast Guard with a visible presence out in the seaport that may deter a potential terrorist attack from being carried out.

As the lead federal agency responsible for protecting the U.S. maritime domain, the Coast Guard has spearheaded an interagency approach for establishing maritime domain awareness. Within this approach are several activities and actions intended to collect information and intelligence, analyze the information and intelligence, and disseminate the analyzed information and intelligence to appropriate federal, state, local, or private seaport stakeholders. Some of these actions were required under MTSA, such as the establishment of an Automatic Identification System to track vessels, as well as creation of area maritime security committees of local seaport stakeholders who identify and address risks within their seaport. In addition to these actions, the Department of Defense and DHS formed a Maritime Domain Awareness Senior Steering Group in 2004 to coordinate national efforts to improve maritime domain awareness. Under Homeland Security Presidential Directive 13, issued in December 2004, this steering group is required to develop a national plan for maritime domain awareness by June 2005. According to the head of the Coast Guard's maritime domain awareness program, a draft of this plan is being reviewed before it is submitted to the President. Table 3 shows some of the actions currently being taken or underway to enhance maritime domain awareness.

Table 3: Examples of Activities to Develop Maritime Domain Awareness

Maritime Domain Awareness activity	Example of activity
Collection of information and intelligence	**Automatic Identification System:** AIS uses a device aboard a vessel to transmit an identifying signal to a receiver located at the seaport and other ships in the area. This signal gives seaport officials and other vessels nearly instantaneous information and awareness about a vessel's identity, position, speed, and course. The Coast Guard intends to provide AIS coverage to meet maritime domain awareness requirements in all navigable waters of the United States and further offshore. As of May 2005, the Coast Guard has AIS coverage in several seaports and coastal areas.[a] In addition to this system, the Coast Guard is also working with the International Maritime Organization (IMO) to develop functional and technical requirements for long-range tracking out to 2,000 nautical miles. The Coast Guard proposed an amendment to the International Convention for Safety of Life at Sea (SOLAS) for this initiative, which is currently under consideration by the international body. However, according to the Coast Guard, the issue of long-range tracking is contentious internationally and it is uncertain whether the amendment will be adopted.
Analysis of information and intelligence	**Maritime Intelligence Fusion Centers and Field Intelligence Support Teams:** Centers have been established by the Coast Guard on the East and West Coasts to provide actionable intelligence to Coast Guard commanders and units. The teams also conduct initial analysis of intelligence in coordination with federal, state, and local law enforcement and intelligence agencies.
Dissemination of information and intelligence	**Area Maritime Security Committees:** The committees serve as forums for local seaport stakeholders from federal agencies, state and local governments, law enforcement, and private industries to gain a comprehensive perspective of security issues at a seaport location. Information is disseminated through regularly scheduled meetings, issuance of electronic bulletins on suspicious activities around seaport facilities, and sharing key documents. The committees also serve as a link for communicating threats and security information to seaport stakeholders. **Interagency Operational Centers:** These centers provide information 24 hours a day about maritime activities and involve various federal and nonfederal agencies directly in operational decisions using this information. Radar, sensors, and cameras offer representations of vessels and facilities. Other data are available from intelligence sources, including data on vessels, cargo, and crew. Unlike the area maritime security committees, these centers are operational in nature with a unified or joint command structure designed to receive information and act on it. Representatives from the various agencies work side by side, each having access to databases and other sources of information from their respective agencies. These currently exist in three locations: Charleston, South Carolina; Norfolk, Virginia; and San Diego, California.

Source: GAO analysis of Coast Guard data.

[a] The Coast Guard currently has AIS coverage in the following areas: Alaska (Anchorage, Homer, Nikiski, Seward, Valdez, and Juneau); Puget Sound (Seattle, Tacoma, Everett, Port Angeles, and Olympia); the Columbia River entrance; San Francisco Bay and approaches; Los Angeles-Long Beach Harbor and approaches; San Diego and approaches; Hawaii (Honolulu and Pearl Harbor); Gulf of Mexico (Houston-Galveston, Port Arthur, Berwick Bay, and Lower Mississippi River-New Orleans-Baton Rouge); South Florida (Key West, Miami, and Port Everglades); Charleston, South Carolina; Norfolk, Virginia; New York, New York; Long Island Sound (New Haven and New London); Boston Harbor and approaches; and Sault Ste. Marie, Michigan.

While many of the activities to develop maritime domain awareness are still underway, some progress has already been made. One activity in this area that we have recently looked at concerns the process of information sharing between federal and nonfederal seaport stakeholders participating on area maritime security committees.[6] The Coast Guard organized 43 of these committees, covering the nation's 361 seaports. While a primary purpose of the committees is to develop a seaport-wide security plan for their respective seaports, the committees also provide links for communicating threats and security information to seaport stakeholders—links that generally did not exist prior to the creation of the committees. The types of information shared among committee members with security clearances included assessments of vulnerabilities at specific seaport locations, information about potential threats or suspicious activities, and strategies to use in protecting key infrastructure. Our review found that the committees improved information sharing among seaport security stakeholders, including the timeliness, completeness, and usefulness of information shared.

Another aspect of improving maritime domain awareness involves having the assets to communicate and conduct patrols, and in this regard, the Coast Guard has budgeted for and is in the process of receiving substantial new resources. In 1996, the Coast Guard initiated a major recapitalization effort—known as the Integrated Deepwater System—to replace and modernize the agency's aging and deteriorating fleet of aircraft and vessel assets. The focus of the program is not just on new ships and aircraft, but also on newer, more capable assets, with improved and integrated command, control, communications and computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities. Although the program was started before the attacks of September 11, 2001, the Coast Guard plans to leverage these capabilities of the 20 year, $17 billion dollar program to enhance its maritime domain awareness and seaport security operations such as patrols and response.

Challenges for Improving Maritime Security Take Three Main Forms

Propelled by a strong sense of urgency to secure the seaports, federal agencies, such as the Coast Guard, CBP, and TSA, accomplished a considerable amount in a short time. At the same time, these actions have also shown the strains that often occur when difficult tasks must be done quickly. We have not examined every action that has been started or enhanced regarding maritime security, but our work to date has covered a number of them. It is not surprising that we have found, besides the

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

progress made, a number of missteps, false starts, and inefficiencies. These represent challenges to overcome.

While some of these challenges will be resolved with time, analysis, and oversight, there are other challenges that bear even more careful watching, because they may prove to be considerably more difficult to overcome. I would like to highlight three of those challenges, providing examples from our recent work. These three challenges involve (1) design and implementing programs, (2) coordinating between different agencies and stakeholder interests, and (3) determining how to pay for these efforts.

Challenges in Program Design and Implementation

I will discuss today two illustrative examples related to challenges in program design and implementation that we have identified from our work. These include the (1) lack of planning and performance measures for program design and (2) lack of experienced personnel for program implementation.

Lack of Planning and Performance Measures for Program Design

One effect of having to design programs quickly is that they may lack such elements as strategic plans and performance measures needed to set program goals and monitor performance. The lack of such tools can create problems that need to be resolved as the program unfolds. For example, we have reviewed CBP's actions to establish a system meant to reliably identify potentially risky cargo containers.

Our work has shown that a need exists for additional efforts in several homeland security activities, including securing cargo, in order to help ensure the effectiveness of the approach.[7] As we noted in a July 2003 report, the former U.S. Customs Service, part of which is now CBP initiated the Container Security Initiative (CSI) in January 2002 in response to security vulnerabilities created by ocean container trade and the concern that terrorists could exploit these vulnerabilities to transport or detonate WMDs in the United States. [8] During the first year, program

[7] GAO, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*, GAO-03-770 (Washington, D.C.: July 2003); and GAO, *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T (Washington, D.C.: March 2004). In addition, we have additional work underway regarding the Container Security Initiative program and expect to issue our report in May.

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

officials quickly designed and rolled out the initiative, modifying operations over time. The service achieved strong initial participation among the countries that it sought to enroll in the initiative, reaching agreement with 15 governments to place U.S. personnel at 24 seaports, and placing teams in 5 of these seaports. However, CBP had not taken adequate steps to incorporate human capital planning, develop performance measures, and plan strategically—factors essential to the program's long-term success and accountability. We noted, for example, that:

- More than 1 year into the implementation of the initiative, CBP had not developed a systematic human capital plan to recruit, train, and assign the more than 120 program staff that would be needed for long-term assignments in a wide range of foreign seaports, some of which could require language capabilities and diplomatic skills.

- CBP lacked performance measures for the initiative that demonstrated program achievements and established accountability. For example, the service lacked measures that assessed the impact of collocating U.S. and foreign customs officials in foreign seaports to determine which containers should be targeted for inspection.

- CBP's focus on short-term operational planning in order to quickly implement the program impeded its ability to systematically carry out strategic planning. We noted that the service did not have a strategic plan for the initiative that describes how it intends to achieve program goals and objectives. As a result, CBP lacked elements of strategic planning that would improve the management of the program and allow CBP to establish accountability for planned expenditures.

As also reported in July 2003, another program that did not take adequate steps to incorporate the human capital planning and performance measures necessary for the program's long-term success and accountability is CBP's Customs-Trade Partnership Against Terrorism (C-TPAT) program. Initiated in November 2001, C-TPAT is an initiative that attempts to improve the security of the international supply chain. It is a cooperative program between CBP and members of the international trade community in which private companies agree to improve the security of their supply chains in return for a reduced likelihood that their containers will be inspected.

During the first year, more than 1,700 companies agreed to participate in the program, and most received the key benefit—a reduced likelihood of inspections for WMDs. However, we noted similar kinds of problems to those in the CSI program. For example, we found that:

- Even as it rolled out new program elements, CBP lacked a human capital plan for increasing the number of C-TPAT staff from 10 to more than 160.

- CBP had not developed performance measures for C-TPAT that would establish accountability and measure program achievements. For example, CBP had no performance measure to assess the impact of C-TPAT on improving supply chain security practices, possibly resulting in benefits being granted to undeserving companies.

- CBP lacked strategic planning in rolling out C-TPAT, failing to communicate how it planned to implement critical program elements designed to verify that companies have security measures in place and follow through with recommended changes.

We are currently reviewing both the CSI and CTPAT programs and will soon be issuing reports to update our earlier evaluation of these programs.

Lack of Experienced Personnel for Program Implementation

One major challenge in program implementation is the lack of experienced personnel, which is to be expected given the rapid increase in newly hired personnel since September 11, 2001. Agencies such as the Coast Guard expect to see large increases in the number of staff over the next few years to help meet new and expanded responsibilities. Consequently, they also face a challenge in absorbing this increase and training them to be fully productive. We pointed out early on that this would be a challenge for the Coast Guard,[9] and subsequent work has shown this to be the case. For example, after a Coast Guard internal review found that readiness of its multi-mission stations—the shore-based units whose responsibilities include finding and rescuing mariners in danger--had been in decline for an extended period, the Coast Guard began efforts to improve the readiness of the stations. This effort was complicated by the new homeland security responsibilities the stations assumed after the terrorist attacks of September 11, 2001. In a recent review of staffing and readiness at these multi-mission stations,[10] we found that the Coast Guard was still in the

[9] GAO, *Homeland Security: Challenges Facing the Coast Guard as It Transitions to the New Department*, GAO-03-467T (Washington, D.C.: February 2003).

[10] GAO, *Coast Guard: Station Readiness Improving, but Resource Challenges and Management Concerns Remain*, GAO-05-161 (Washington, D.C.: Jan. 31, 2005).

process of defining new standards for security activities and had yet to translate the impact of security-related mission responsibilities into specific station readiness requirements, such as staffing standards. Consequently, even though station staffing had increased 25 percent since 2001, the Coast Guard was unable to align staffing resources with mission activities, which resulted in a significant number of positions not being filled with qualified personnel and station personnel working significantly longer hours than are allowed under the Coast Guard's work standards.

We also identified personnel or human capital challenges such as lack of experienced personnel related to the Coast Guard's program to oversee implementation of MTSA-required security plans by owners and operators of maritime facilities and vessels. These security plans are performance-based, meaning the Coast Guard has specified the outcomes it is seeking to achieve and has given seaport stakeholders responsibility for identifying and delivering the measures needed to achieve these outcomes. While this approach provides flexibility to owners and operators in designing and implementing their plans, it also places a premium on the skills and experience of inspectors to identify deficiencies and recommend corrective action. Because the Coast Guard had to review and assess for compliance more than 12,000 security plans for facilities and vessels, it had to rely heavily on reservists, which varied greatly in the level of their skills and experience in this area. For example, some reservists had graduate degrees in security management while others had no formal security training or experience. In June 2004, we recommended that the Coast Guard carefully evaluate its efforts during the initial surge period for inspections.[11] The Coast Guard has adjusted its inspection program to make its compliance assessments more relevant and useful, but it has not yet determined the overall effectiveness of its compliance actions.

Challenges in Coordinating Actions

Coordinating massive new homeland security actions has been an acknowledged challenge since the events of September 11, 2001, and seaport security has been no exception. On the federal side alone, we have for several years designated implementing and transforming the new DHS as a high-risk area.[12] Since the agency's inception in March 2003, DHS leadership has provided a foundation to maintain critical operations while

[11] GAO, *Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security*, GAO-04-838 (Washington, D.C.: June 30, 2004).

[12] GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: Jan. 2005).

undergoing transformation, and the agency has begun to put systems in place to operate more effectively and efficiently as an agency. In managing its transformation, however, DHS still faces such issues as forming effective partnerships with other governmental and private-sector entities.

We have made numerous recommendations related to information sharing, particularly as it relates to fulfilling federal critical infrastructure protection responsibilities.[13] For example, we have reported on the practices of organizations that successfully share sensitive or time-critical information, including establishing trust relationships, developing information-sharing standards and protocols, establishing secure communications mechanisms, and disseminating sensitive information appropriately. Federal agencies such as DHS and the Coast Guard have concurred with our recommendations that they develop appropriate strategies to address the many potential barriers to information sharing. However, as of January 2005, many federal efforts to do this remain in the planning or early implementation stages especially in the area of homeland security information sharing, including establishing clear goals, objectives, and expectations for the many participants in information-sharing efforts; and consolidating, standardizing, and enhancing federal structures, policies, and capabilities for the analysis and dissemination of information. In this regard, the issue of information-sharing across agency and stakeholder lines has emerged as a significant enough challenge that we have also designated it as a high-risk area. Here are three examples that illustrate the kinds of problems and challenges that remain related to seaport security.

Obtaining Security Clearances

While coordination of information-sharing at the seaport level appears to have improved, seaports are experiencing challenges with regards to nonfederal officials obtaining security clearances. For some time, state and local seaport and law enforcement personnel have reported problems in obtaining federally generated intelligence information about their jurisdictions because they did not have a federal security clearance. However, as of February 2005—over 4 months after the Coast Guard had developed a list of over 350 nonfederal area maritime security committee participants as having a need for a security clearance—only 28 had submitted the necessary paperwork for the background check. Local

[13] GAO, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, GAO-03-1165T (Washington, D.C.: Sept. 17, 2003); and *Homeland Security: Information-Sharing Responsibilities, Challenges, and Key Management Issues*, GAO-03-715T (Washington, D.C.: May 8, 2003).

Coast Guard officials told us they did not clearly understand their responsibility for communicating with state and local officials about the process for obtaining a security clearance. After we expressed our concerns to Coast Guard officials in headquarters in February 2005, officials took action and drafted guidelines clarifying the role that local Coast Guard officials play in the program.

Sharing Information about Security Exercises

In a January 2005 report,[14] we reported that improvement in the coordination of state, local, and federal entities during seaport exercises was needed. While it was still too early to determine how well entities will function in coordinating an effective response to a seaport-related threat or incident, we identified four operational issues that needed to be addressed in order to promote more effective coordination. We found that more than half of the seaport exercises and after-action reports we examined raised communication issues, including problems with information sharing among first responders and across agency lines. We also found that over half of the exercises raised concerns with communication and the resources available, including inadequate facilities or equipment, differing response procedures, and the need for additional training in joint agency response. To a lesser extent, we found concerns with participants' ability to coordinate effectively and know who had the proper authority to raise security levels, board vessels, or detain passengers.

Developing a Transportation Worker Identification Credential

Beyond information-sharing, a host of challenges remain in coordinating across agency lines and in resolving issues that cut across a wide range of stakeholder perspectives. In this regard, there is perhaps no better example in our recent work than the delayed attempts to develop a major component of the security framework envisioned under MTSA—an identification card for maritime workers. The transportation worker identification credential (TWIC) was initially envisioned by TSA before it became part of DHS to be a universally recognized identification card accepted across all modes of the national transportation system, including airports, seaports, and railroad terminals, using biological metrics, such as fingerprints, to ensure individuals with such an identification card had undergone an assessment verifying that they do not pose a terrorism security risk. TSA initially projected that it would test a prototype of such a card system in 2003 and issue the first of the cards in August 2004. After

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

TSA became part of DHS, testing of the prototype was delayed because of the difficulty in obtaining a response from DHS policy officials who also subsequently directed the agency to reexamine additional options for issuing the identification card. In addition to coordinating within DHS, TSA has had to coordinate with over 800 national level transportation-related stakeholders. Several stakeholders at seaports and seaport facilities told us that, while TSA solicited their input on some issues, TSA did not respond to their input or involve them in making decisions regarding eligibility requirements for the card.[15] In particular, some stakeholders said they had not been included in discussions about which felony convictions should disqualify a worker from receiving a card, even though they had expected and requested that DHS and TSA involve them in these decisions. Obtaining stakeholder involvement is important because achieving program goals hinges on the federal government's ability to form effective partnerships among many public and private stakeholders. If such partnerships are not in place—and equally important, if they do not work effectively—TSA may not be able to test and deliver a program that performs as expected. Until TSA and DHS officials agree on a comprehensive project plan to guide the remainder of the project and work together to set and complete deadlines, and TSA can effectively manage its stakeholders' interests, it may not be able to successfully develop, test, and implement the card program. We issued a report on TWIC in December 2004[16] and the Senate Committee on Homeland Security and Governmental Affairs has asked us to review the program again.

Challenges in Providing Funding for Seaport Security Actions and Initiatives

Our reviews indicate that funding is a pressing challenge to putting effective seaport security measures in place and sustaining these measures over time. This is the view of many transportation security experts, industry representatives, and federal, state, and local government officials with whom we have spoken. While some security improvements are inexpensive, most require substantial and continuous funding. For example, a preliminary Coast Guard estimate placed the cost of

[15] Of the facilities testing TSA's prototype, we visited ports and facilities in the Delaware River Region, including Wilmington Port Authority, the Philadelphia Maritime Exchange, and the South Jersey Port. We also visited ports and facilities on the West Coast, including those in the Port of Seattle, Port of Los Angeles, and Port of Long Beach as well as ports and facilities in Florida, including Port Everglades and the Port of Jacksonville.

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

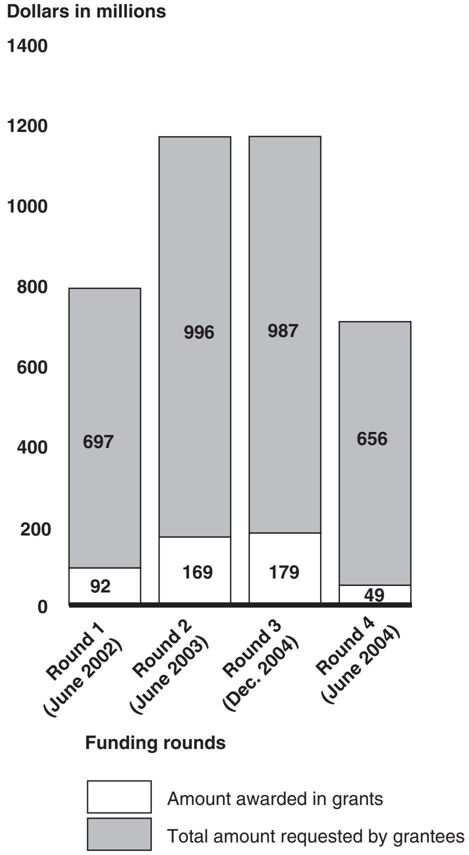
implementing the International Maritime Organization security code and the security provisions in MTSA at approximately $1.5 billion for the first year and $7.3 billion over the succeeding decade. This estimate should be viewed more as a rough indicator than a precise measure of costs, but it does show that the cost is likely to be substantial.[17]

At the federal level, more than $560 million in grants has been made available to seaports, localities, and other stakeholders since 2002 under the Port Security Grant Program and the Urban Area Security Initiative. The purpose of these programs was to reduce the vulnerability of seaports to potential terrorist attacks by enhancing facility and operation security. The programs funded several projects, including security assessments; physical enhancements, such as gates and fences; surveillance equipment, such as cameras; and the acquisition of security equipment, such as patrol vessels or vehicles. Awardees have included seaport authorities, local governments, vessel operators, and private companies with facilities in seaport areas. Interest in receiving port security grants has been strong, and, as figure 2 shows, applicant requests have far exceeded available funds. We are currently examining the Port Security Grant Program at the request of several Members of Congress, and we are focusing this review on the risk management practices used in comparing and prioritizing applications. Our work is under way, and we expect to issue our report later this year.[18]

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

[18] DHS has proposed consolidating homeland grant programs into a single program. Known as the Targeted Infrastructure Protection Program (TIPP), the program would lump together grant funding for transit, port security and other critical infrastructure, and eliminate specific grant programs for port, rail, truck, intercity bus, and nongovernmental organizations security. In its fiscal year 2006 budget request, the administration proposed $600 million for TIPP, a $260-million increase in overall funding from fiscal year 2005 for the specific transportation security grant programs. In fiscal year 2005, funding for port, rail, truck, intercity bus, and non-governmental organizations security totaled $340 million.

Figure 2: Comparison of Requests and Awards for Funding, Port Security Grant Program, Fiscal Years 2002-2004



Source: GAO analysis of TSA data.

Note: Figure 2 does not include $75 million that was awarded to 14 high-risk seaport areas under the Urban Area Security Initiative (UASI) by the Office of Domestic Preparedness. This program is separate from its basic UASI program, which provided formula grants to 50 urban areas for equipment, training, planning, exercise, operational needs, and critical infrastructure.

Where the money will come from for all of the funding needs is unclear. In our 2002 statement on national preparedness,[19] we highlighted the need to examine the sustainability of increased funding not only for seaport security, but for homeland security efforts in general. The current economic environment makes this a difficult time for private industry and

[19] GAO, *National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts Is Critical to an Effective National Strategy for Homeland Security*, GAO-02-621T (Washington, D.C.: April 2002).

state and local governments to make security investments and sustain increased security costs. According to industry representatives and experts we contacted, most of the transportation industry operates on a very thin profit margin, making it difficult to pay for additional security measures. Budgetary and revenue constraints, coupled with increasing demands on resources, makes it more critical that federal programs be designed carefully to match the priorities and needs of all partners—federal, state, local, and private—and provide the greatest results for the expenditure.

Setting Performance Goals and Measures and Assessing Risk Are Important Next Steps

The final purpose of my testimony today is to offer observations, based on the work we have done to date, about important next steps for decision makers in charting a course for future actions. The terrorist attacks of September 11, 2001, evoked with stunning clarity the face and intent of enemies very different from those the nation has faced before—terrorists such as al Qaeda, willing and able to attack us in our territory using tactics designed to take advantage of our relatively open society and individual freedoms. The amount of activity in response has been considerable, and although there have been no serious incidents in the United States in the interim, the threat of terrorism will likely persist well into the 21st century. Thus, it is important to continue to make progress in our efforts. Beyond addressing the kinds of challenges discussed above, however, two other matters stand out. One involves developing a better understanding of how much progress has actually been made to secure our seaports; the other involves developing a better strategy to manage risk and prioritize what areas need further progress and how resources can be best allocated.

Lack of Goals and Measures Makes Determining Progress Difficult

Although there is widespread agreement that actions taken so far have led to a heightened awareness of the need for security and an enhanced ability to identify and respond to many security threats, it is difficult to translate these actions into a clear sense of how far we have progressed in making seaports more secure. One reason is that seaport security efforts, like homeland security efforts in general, lack measurable goals, as well as performance measures to measure progress toward those goals. As others such as the Gilmore Commission have stated, a continuing problem for homeland security has been the lack of clear strategic guidance about the definition and objectives of preparedness.[20] For example, the Coast Guard has a set of performance indicators for each of its nonsecurity missions. It regularly reports on how well it is doing in rescuing mariners at sea, interdicting foreign fishing boats attempting to fish the in U.S. exclusive economic zone, or maintaining aids to navigation on the nation's waterways. However, although it has been more than 3 years since the September 11, 2001, attacks, the Coast Guard is still in the process of developing a performance indicator for its seaport security activities that can be used to indicate what progress has been made to secure seaports. Completion of this indicator and careful tracking of it over the long term is essential to help ensure that taxpayer dollars are being spent wisely to make seaports more secure. Similarly, as discussed earlier in describing the actions taken to secure the cargo transiting through seaports in containers, performance measures are needed to determine the progress such actions are making to reduce vulnerabilities of the international supply chain.

A challenge exists in measuring progress in this area, because seaport security, like many aspects of homeland security, relies upon the coordinated actions of many stakeholders and, in many cases, upon "layers" of defenses. In this regard, we have pointed out that systems and service standards—which focus on the performance, design, and overall management of processes and activities—hold great potential to improve coordination across such dimensions and enhance measurement of continued preparedness.[21] While such standards are already being used in many parts of the private sector, creation of performance and results measures for national security in general, and seaport security in particular, remains a work in progress.

Risk Management Is an Essential Tool for Focusing Efforts Effectively

Even with clear goals and effective performance measures, it seems improbable that all risk can be eliminated, or that any security framework can successfully anticipate and thwart every type of potential terrorist threat that highly motivated, well skilled, and adequately funded terrorist groups could think up. This is not to suggest that security efforts do not

[20] The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *V. Forging America's New Normalcy* (Arlington, VA: Dec. 15, 2003).

[21] GAO, *Homeland Security: Observations on the National Strategies Related to Terrorism*, GAO-04-1075T (Washington, D.C.: Sept. 22, 2004).

matter—they clearly do. However, it is important to keep in mind that total security cannot be bought no matter how much is spent on it. We cannot afford to protect everything against all threats—choices must be made about security priorities. Thus, great care needs to be taken to assign available resources to address the greatest risks, along with selecting those strategies that make the most efficient and effective use of resources.

One approach to help ensure that resources are assigned and appropriate strategies are selected to address the greatest risks is through risk management—that is, defining and reducing risk. A risk management approach is a systematic process for analyzing threats and vulnerabilities, together with the criticality (that is, the relative importance) of the assets involved. This process consists of a series of analytical and managerial steps, basically sequential, that can be used to assess vulnerabilities, determine the criticality (that is, the relative importance) of the assets being considered, determine the threats to the assets, and assess alternatives for reducing the risks. Once these are assessed and identified, actions to improve security and reduce the risks can be chosen from the alternatives for implementation. To be effective, however, this process must be repeated when threats or conditions change to incorporate any new information to adjust and revise the assessments and actions.

Some elements of risk management have been incorporated into seaport security activities. For example, to meet the requirements of MTSA, security plans for seaports, facilities, and vessels have been developed based on assessments that identify their vulnerabilities. In addition, the Coast Guard is using the Port Security Risk Assessment Tool, which is designed to prioritize risk according to a combination of possible threat, consequence, and vulnerability. Under this approach, seaport infrastructure that is determined to be both a critical asset and a likely and vulnerable target would be a high priority for security enhancements or funding. By comparison, infrastructure that is vulnerable to attack but not as critical or infrastructure that is very critical but already well protected would be lower in priority. In a homeland security setting, possible uses of data produced from risk management efforts include informing decisions on where the federal government might spend billions of dollars within and between federal departments, as well as informing decisions on grants awarded to state and local governments.

As the nation moves ahead with seaport security efforts, there are plans to incorporate risk management as part of the nation's larger homeland security strategy. Homeland Security Presidential Directive 7, issued in

December 2003, charged DHS with integrating the use of risk management into homeland security activities. The directive called on the Department to develop policies, guidelines, criteria, and metrics for this effort. To meet this requirement, the Coast Guard has taken steps to use risk management in prioritizing the protection of key infrastructure within and between seaports. We are currently in the process of assessing the progress the Coast Guard has made in these efforts. In addition, we are reviewing the extent to which a risk management approach is being used by other DHS agencies, such as the Information Analysis and Infrastructure Protection Directorate, to evaluate the relative risk faced by key infrastructure within seaports and across broad sectors of national activity, such as seaports and aviation, to help ensure funding and resources are allocated to where they are needed most. Our work is still under way and not far enough along to discuss at this time. It is likely, however, that attention to risk management will be a key part of the ongoing dialogue about the nation's homeland security actions in general, and its seaport security actions in particular.

Concluding Observations

Managing the risks associated with securing our nation's seaports involves a careful balance between the benefits of added security and the potential economic impacts of security enhancements. While there is broad support for greater security, the national economy is heavily dependent on keeping goods, trucks, trains, and people flowing quickly through seaports, and bringing commerce to a crawl in order to be completely safe carries its own serious economic consequences. Striking the right balance between increased security and protecting economic vitality is an important and difficult task. Considering this, three things stand out as important from the work we have conducted:

- Seaports are not retreating as a homeland security issue. They are an attractive terrorist target and are likely to remain so, because by their nature they represent a vulnerability that is always open to potential exploitation.

- Seaport security has lived up to its billing as an area in which security measures can be difficult to implement. The range of activity in seaport areas can be extremely wide, as can the range of stakeholders and the fragmentation of responsibility among them. Many of the problems we have identified with individual programs and efforts can likely be overcome with time and effort, but success is not assured. We are already seeing some efforts, such as the TWIC identification card, becoming deeply mired in problems. These activities will thus continue to demand close attention.

- The national dialogue on this issue is likely to focus increasingly in trying to determine what we are getting for our efforts and where we should invest the dollars we have. Therefore, it is critical that federal programs be designed carefully to try to match the priorities and needs of all partners—federal, state, local, and private—and use performance measures to effectively allocate funds and resources. On this point, there is work to do, because agencies such as the Coast Guard currently lack a systematic approach for explaining the relationship between the expenditure of resources and performance results in seaport security, limiting its ability to critically examine its resource needs and prioritize program efforts. Providing answers also requires an ability to carefully assess what the key vulnerabilities are and what should be done to protect them. Only by doing this will we have reasonable assurance that we are doing the best job with the dollars we have.

Mr. Chairman, this concludes my prepared statement. I would be pleased to answer any questions that you or other Members of the Committee may have.

Contacts and Acknowledgments

For information about this testimony, please contact Margaret Wrightson, Director, Homeland Security and Justice Issues, at (415) 904-2200, or wrightsonm@gao.gov. Other individuals making key contributions to this testimony include Steve Calvo, Geoffrey Hamilton, Christopher Hatscher, Sara Margraf, and Stan Stenersen.

Appendix I: Related GAO Products

Coast Guard: Preliminary Observations on the Condition of Deepwater Legacy Assets and Acquisition Management Challenges. GAO-05-307T. Washington, D.C.: April 20, 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 31, 2005.

Coast Guard: Observations on Agency Priorities in Fiscal Year 2006 Budget Request. GAO-05-364T. Washington, D.C.: March 17, 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: Planning Needed to Develop and Operate Maritime Worker Identification Card Program. GAO-05-106. Washington, D.C.: December 10, 2004.

Maritime Security: Better Planning Needed to Help Ensure an Effective Port Security Assessment Program. GAO-04-1062. Washington, D.C.: September 30, 2004.

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

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

Coast Guard: Deepwater Program Acquisition Schedule Update Needed. GAO-04-695. Washington, D.C.: June 14, 2004.

Coast Guard: Key Management and Budget Challenges for Fiscal Year 2005 and Beyond. GAO-04-636T. Washington, D.C.: April 7, 2004.

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

Coast Guard Programs: Relationship between Resources Used and Results Achieved Needs to Be Clearer. GAO-04-432. Washington, D.C.: March 22, 2004.

Contract Management: Coast Guard's Deepwater Program Needs Increased Attention to Management and Contractor Oversight. GAO-04-380. Washington, D.C.: March 9, 2004.

Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers. GAO-04-325T. Washington, D.C.: December 16, 2003.

Posthearing Questions Related to Aviation and Port Security. GAO-04-315R. Washington, D.C.: December 12, 2003.

Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain. GAO-03-1155T. Washington, D.C.: September 9, 2003.

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

Homeland Security: Challenges Facing the Department of Homeland Security in Balancing Its Border Security and Trade Facilitation Missions. GAO-03-902T. Washington, D.C.: June 16, 2003.

Coast Guard: Challenges during the Transition to the Department of Homeland Security. GAO-03-594T. Washington, D.C.: April 1, 2003.

Transportation Security: Post-September 11th Initiatives and Long-Term Challenges. GAO-03-616T. Washington, D.C.: April 1, 2003.

Coast Guard: Comprehensive Blueprint Needed to Balance and Monitor Resource Use and Measure Performance for All Missions. GAO-03-544T. Washington, D.C.: March 12, 2003.

Homeland Security: Challenges Facing the Coast Guard as It Transitions to the New Department. GAO-03-467T. Washington, D.C.: February 12, 2003.

Container Security: Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges. GAO-03-297T. Washington, D.C.: November 18, 2002.

Coast Guard: Strategy Needed for Setting and Monitoring Levels of Effort for All Missions. GAO-03-155. Washington, D.C.: November 12, 2002.

Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful. GAO-02-993T. Washington, D.C.: August 5, 2002.

Combating Terrorism: Preliminary Observations on Weaknesses in Force Protection for DOD Deployments through Domestic Seaports. GAO-02-955TNI. Washington, D.C.: July 23, 2002.

Appendix II: Previous GAO Recommendations

Agency/program	GAO recommendations
Coast Guard	***GAO Recommendations to the U.S. Coast Guard***
Automatic Identification System (AIS)	• To seek and take advantage of opportunities to partner with organizations willing to develop AIS systems at their own expense in order to help reduce federal costs and speed development of AIS nationwide. (GAO-04-868)
Deepwater acquisition	• Take the necessary steps to make integrated product team (IPT) members effective, including (1) training IPTS in a timely manner, (2) chartering the sub-IPTs, and (3) making improvements to the electronic information system that would result in better information sharing among IPT members who are geographically dispersed. (GAO-04-380) • Follow the procedures outlined in the human capital plan to ensure that adequate staffing is in place and turnover among Deepwater personnel is proactively addressed. (GAO-04-380) • Ensure that field operators and maintenance personnel are provided with timely information and training on how the transition will occur and how maintenance responsibilities are to be divided between system integrator and Coast Guard personnel. (GAO-04-380) • Develop and adhere to measurable award fee criteria consistent with the Office of Federal Procurement Policy's guidance. (GAO-04-380) • Ensure that the input of contracting officer's technical representatives (COTR) is considered and set forth in a more rigorous manner. (GAO-04-380) • Hold the system integrator accountable in future award fee determinations for improving the effectiveness of IPTs. (GAO-04-380) • Establish a time frame for when the models and metrics will be in place with the appropriate degree of fidelity to be able to measure the contractor's progress toward improving operational effectiveness. (GAO-04-380) • Establish a total ownership cost (TOC) baseline that can be used to measure whether the Deepwater acquisition approach is providing the government with increased efficiencies compared to what it would have cost without this approach. (GAO-04-380) • Establish criteria to determine when the TOC baseline should be adjusted and ensure that the reasons for any changes are documented. (GAO-04-380) • Develop a comprehensive plan for holding the system integrator accountable for ensuring an adequate degree of competition among second-tier suppliers in future program years. This plan should include metrics to measure outcomes and consideration of how these outcomes will be taken into account in future award fee decisions. (GAO-04-380) • For subcontracts over $5 million awarded by Integrated Coast Guard Systems LLC (ICGS) to Lockheed Martin and Northrop Grumman, require Lockheed Martin and Northrop Grumman to notify the Coast Guard of a decision to perform the work themselves rather than contracting it out. (GAO-04-380) • To update the original 2002 Deepwater acquisition schedule in time to support the fiscal year 2006 Deepwater budget submission to DHS and Congress and at least once a year thereafter to support each budget submission, which should include the current status of asset acquisition phases, interim phase milestones, and the critical paths linking the delivery of individual components to particular assets. (GAO-04-695)

Agency/program	GAO recommendations
MTSA security plans	• Conduct a formal evaluation of compliance inspection efforts taken during the initial 6-month surge period, including the adequacy of security inspection staffing, training, and guidance, and use this evaluation as a means to strengthen the compliance process for the longer term. (GAO-04-838) • Clearly define the minimum qualifications for inspectors and link these qualifications to a certification process. (GAO-04-838) • Consider including unscheduled and unannounced inspections and covert testing as part of its inspection strategy to provide better assurance that the security environment at the nation's seaports meets the nation's expectations. (GAO-04-838)
Multi-mission station readiness	• Revise the *Boat Forces Strategic Plan* to (1) reflect the impact of homeland security requirements on station needs and (2) identify specific actions, milestones, and funding needs for meeting those needs. (GAO-05-161) • Develop measurable annual goals for stations. (GAO-05-161) • Revise the processes and practices for estimating and allocating station personal protection equipment (PPE) funds to reliably identify annual funding needs and use this information in making future funding decisions. (GAO-05-161)
Obtaining security clearances	• Develop formal procedures so that local and headquarters officials use the Coast Guard's internal databases of state, local, and industry security clearances for area maritime committee members as a management tool to monitor who has submitted applications for a security clearance and to take appropriate action when application trends point to possible problems. (GAO-05-394) • Raise awareness of state, local, and industry officials about the process of applying for security clearances. (GAO-05-394)
Port security assessment program	• To define and document the geographic information system (GIS) functional requirements. (GAO-04-1062) • Develop a long-term project plan for the GIS and the Port Security Assessment Program as a whole (including cost estimates, schedule, and management responsibilities). (GAO-04-1062)
Resource effectiveness	• To develop a time frame for expeditiously proceeding with plans for implementing a system that will accurately account for resources expended in each of its program areas. (GAO-04-432) • Ensure that the strategic planning process and its associated documents include a strategy for (1) identifying intervening factors that may affect program performance and (2) systematically assessing the relationship between these factors, resources used, and results achieved. (GAO-04-432)
Seaport exercises	• To help ensure that reports on terrorism-related exercises are submitted in a timely manner that complies with all Coast Guard requirements, the Commandant of the Coast Guard should review the Coast Guard's actions for ensuring timeliness and determine if further actions are needed. (GAO-05-170)
Department of Energy	***GAO Recommendations to the Department of Energy***
Megaports Initiative	• Develop a comprehensive long-term plan to guide the future efforts of the Initiative that includes, at a minimum, (1) performance measures that are consistent with DOE's desire to install radiation detection equipment at the highest priority foreign seaports, (2) strategies to determine how many and which lower priority ports DOE will include in the Initiative if it continues to have difficulty installing equipment at the highest priority ports, (3) projections of the anticipated funds required to meet the Initiative's objectives, and (4) specific time frames for effectively spending program funds. (GAO-05-375) • Evaluate the accuracy of the current per port cost estimate of $15 million, make any necessary adjustments to the Initiative's long-term cost projection, and inform Congress of any changes to the long-term cost projection for the Initiative. (GAO-05-375)

Agency/program	GAO recommendations
U.S. Customs and Border Protection	***GAO recommendations to the U.S. Customs and Border Protection***
Container Security Initiative (CSI) and Customs-Trade Partnership Against Terrorism (C-TPAT)	• Develop *human capital plans* that clearly describe how CSI and C-TPAT will recruit, train, and retain staff to meet their growing demands as they expand to other countries and implement new program elements. These plans should include up-to-date information on CSI and C-TPAT staffing and training requirements and should be regularly used by managers to identify areas for further human capital planning, including opportunities for improving program results. (GAO-03-770) • Expand efforts already initiated to develop *performance measures* for CSI and C-TPAT that include outcome-oriented indicators. These measures should be tangible, measurable conditions that cover key aspects of performance and should enable agencies to assess accomplishments, make decisions, realign processes, and assign accountability. Furthermore, the measures should be used to determine the future direction of these Customs' programs. (GAO-03-770) • Develop strategic plans that clearly lay out CSI and C-TPAT goals, objectives, and detailed implementation strategies. These plans should not only address how the strategies and related resources, both financial and human, will enable Customs to secure ocean containers bound for the United States, but also reinforce the connections between these programs' objectives and both Customs' and the Department of Homeland Security's long-term goals. (GAO-03-770) • Use its resources to maximize the effectiveness of its automated targeting strategy to reduce the uncertainty associated with identifying cargo for additional inspection. (GAO-04-557T) • Institute a national inspection reporting system. (GAO-04-557T) • Test and certify CBP officials that receive the targeting training. (GAO-04-557T) • Resolving the safety concerns of longshoremen unions. (GAO-04-557T)
Transportation Security Administration	***GAO recommendations to the U.S. Transportation Security Administration***
Transportation worker identification card (TWIC)	• Develop a comprehensive project plan for managing the remaining life of the TWIC project. (GAO-05-106) • Develop specific, detailed plans for risk mitigation and cost-benefit and alternatives analyses. (GAO-05-106)

Source: GAO.

(440400)

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

PRINTED ON ♻ RECYCLED PAPER