United States General Accounting Office

GAO

Testimony

Before the Subcommittee on National Security,
Veterans Affairs, and International Relations
House Committee on Government Reform

For Release on Delivery
Expected at 1:00 p.m. EDT
Monday
August 5, 2002

# PORT SECURITY

# Nation Faces Formidable Challenges in Making New Initiatives Successful

Statement of JayEtta Z. Hecker
Director, Physical Infrastructure Issues

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to be here in Tampa to discuss issues critical to successful enhancement of seaport security. While most of the early attention following the September 11 terrorist attacks focused on airport security, an increasing emphasis has since been placed on ports. Much of the attention, at least in the media, focuses on the possibility of introducing weapons of mass destruction or other hazardous cargoes into ship cargoes and from there onto America's docks and into its other transportation systems. However, the vast nature and scope of ports like Tampa pose many other kinds of security concerns as well, such as attacks on cruise ships or petrochemical facilities at or near the port. Addressing such concerns is complicated by the sometimes conflicting views of the many stakeholders that are involved in port decisions, including government agencies at the federal, state, and local levels, and thousands of private sector companies.

As you requested, my testimony today focuses on (1) the vulnerabilities of commercial ports, including Tampa; (2) the initiatives taken by federal agencies and other key stakeholders to enhance seaport security; and (3) challenges faced in implementing security-enhancing initiatives. My comments are based on a body of our work undertaken since September 11, 2001,[1] on homeland security and combating terrorism. Our recently completed work on seaport security is based on detailed site reviews of security issues with officials from the Coast Guard, port authorities, and other public and private stakeholder groups. We visited three Florida seaports—including Tampa—and the ports of Charleston, South Carolina, Oakland, California, Honolulu, Hawaii, Boston, Massachusetts, and Tacoma, Washington, selected to reflect geographic dispersion, and risk characteristics. We obtained information on initiatives from officials from Coast Guard headquarters, the Defense Threat Reduction Agency (DTRA),[2] and the Maritime Administration, as well as the American Association of Port Authorities and the private contractor recently hired by the Coast Guard to perform comprehensive port vulnerability assessments. See the appendix for a more detailed explanation of our scope and methodology.

[1] See "Related GAO Products" at the end of this testimony.

[2] DTRA was designated to assist the Chairman of the Joint Chiefs of Staff in fulfilling his responsibilities for force protection by performing vulnerability assessments at Department of Defense installations worldwide. DTRA conducted five assessments at the ports of Baltimore, Honolulu, Guam, Charleston, and Savannah.

In summary:

- Ports are inherently vulnerable to terrorist attacks because of their size, generally open accessibility by water and land, location in metropolitan areas, the amount of material being transported through ports, and the ready transportation links to many locations within our borders. The nation faces a difficult task in providing effective security across the nation's port system, and while progress is being made, an effective port security environment may be many years away. Although some ports have developed in such a way that security can be tightened relatively easily, many ports are extensive in size and have dispersed enterprises intertwined with such security concerns as public roadways and bridges, large petrochemical storage facilities, unguarded access points, and a need for ready access on the part of thousands of workers and customers. The Port of Tampa illustrates many of these same kinds of vulnerabilities, and its proximity to downtown and to other sensitive installations is another reason for concern. While broad popular support exists for greater safety, this task is a difficult one because the nation relies heavily on a free and expeditious flow of goods. To the extent that better security impinges on this economic vitality, it represents a real cost to the system.
- Since September 11, federal agencies, state and local authorities, and private sector stakeholders have done much to address vulnerabilities in the security of the nations ports. The Coast Guard, in particular, has acted as a focal point for assessing and addressing security concerns, anticipating many of the requirements that the Congress and the administration either are contemplating or have already put in place. Two other key federal agencies—the Customs Service and the Immigration and Naturalization Service (INS)—also have actions under way to begin to address such issues as container security and screening of persons seeking entry into the United States. At the state level, Florida has enacted a set of security standards in advance of September 11 and has taken a number of actions to implement these standards at the ports. At other ports across the nation, actions have varied considerably, particularly among private sector stakeholders.
- While the proposal to consolidate federal agencies responsible for border security may offer some long-term benefits, three challenges are central to successful implementation of security enhancing initiatives at the nations ports—standards, funding, and collaboration. The first challenge involves implementing a set of standards that defines what safeguards a port should have in place. Under the Coast Guard's direction, a set of standards is being developed for all U.S. ports to use in conducting port vulnerability assessments. However, many questions remain about whether the thousands of people who have grown accustomed to working in certain

ways at the nation's ports will agree to, and implement, the kinds of changes that a substantially changed environment will require. The second challenge involves determining the amounts needed and sources of funding for the kinds of security improvements that are likely to be required to meet the standards. Florida's experience indicates that security measures are likely to be more expensive than many anticipate, and determining how to pay these costs and how the federal government should participate will present a challenge. The third challenge is ensuring that there is sufficient cooperation and coordination among the many stakeholders to make the security measures actually work. The experience to date indicates that this coordination is more difficult than many stakeholders anticipate and that continued practice and testing will be key in making it work.

## Background

Seaports are critical gateways for the movement of international commerce. More than 95 percent of our non-North American foreign trade (and 100 percent of certain commodities, such as foreign oil, on which we are heavily dependent) arrives by ship. In 2001, approximately 5,400 ships carrying multinational crews and cargoes from around the globe made more than 60,000 U.S. port calls each year. More than 6 million containers (suitable for truck-trailers) enter the country annually. Particularly with "just-in-time" deliveries of goods, the expeditious flow of commerce through these ports is so essential that the Coast Guard Commandant stated after September 11, "even slowing the flow long enough to inspect either all or a statistically significant random selection of imports would be economically intolerable."[3]

This tremendous flow of goods creates many kinds of vulnerability. Drugs and illegal aliens are routinely smuggled into this country, not only in small boats but also hidden among otherwise legitimate cargoes on large commercial ships. These same pathways are available for exploitation by a terrorist organization or any nation or person wishing to attack us surreptitiously. Protecting against these vulnerabilities is made more difficult by the tremendous variety of U.S. ports. Some are multibillion-dollar enterprises, while others have very limited facilities and very little traffic. Cargo operations are similarly varied, including containers, liquid bulk (such as petroleum), dry bulk (such as grain), and iron ore or steel.

[3] *Meeting the Homeland Security Challenge: A Principled Strategy for a Balanced and Practical Response* (September 2001); and *Global Trade: America's Achilles' Heel* (February 2002) by Admiral James M. Loy and Captain Robert G. Ross, U.S. Coast Guard.

Amidst this variety is one relatively consistent complication: most seaports are located in or near major metropolitan areas, where attacks or incidents make more people vulnerable.

The federal government has jurisdiction over harbors and interstate and foreign commerce, but state and local governments are the main port regulators. The entities that coordinate port operations, generally called port authorities, differ considerably from each other in their structure. Some are integral administrative arms of state or local governments; others are autonomous or semi-autonomous self-sustaining public corporations. At least two—The Port Authority of New York and New Jersey and the Delaware River Port Authority—involve two states each. Port authorities also have varying funding mechanisms. Some have the ability to levy taxes, with voter approval required. At other port authorities, voter approval is not required. Some have the ability to issue general obligation bonds, and some can issue revenue bonds. Some ports receive funding directly from the general funds of the governments they are a part of, and some receive state funding support through trust funds or loan guarantees.

A terrorist act involving chemical, biological, radiological, or nuclear weapons at one of these seaports could result in extensive loss of lives, property, and business; affect the operations of harbors and the transportation infrastructure (bridges, railroads, and highways) within the port limits; cause extensive environmental damage; and disrupt the free flow of trade. Port security measures are aimed at minimizing the exploitation or disruption of maritime trade and the underlying infrastructure and processes that support it. The Brookings Institution reported in 2002 that a weapon of mass destruction shipped by container or mail could cause damage and disruption costing the economy as much as $1 trillion.[4] Port vulnerabilities stem from inadequate security measures as well as from the challenge of monitoring the vast and rapidly increasing volume of cargo, persons, and vessels passing through the ports.

Port security is a complex issue that involves numerous key actors including federal, state, and local law enforcement and inspection agencies; port authorities; private sector businesses; and organized labor and other port employees. The routine border control activities of certain

[4] *Protecting the American Homeland: A Preliminary Analysis* by Michael E. O'Hanlon et al., Washington, D.C.: Brookings Institution Press, 2002.

federal agencies, most notably the Coast Guard, Customs Service, and INS, seek to ensure that the flow of cargo, vessels, and persons through seaports complies with all applicable U.S. criminal and civil laws. Also, the Coast Guard, the Federal Bureau of Investigation, the Transportation Security Administration (TSA), and the Department of Defense (DOD) seek to ensure that critical seaport infrastructure is safeguarded from major terrorist attack.

## Characteristics of Many U.S. Ports Leave Them Vulnerable to Terrorist Attacks

While no two ports in the United States are exactly alike, many share certain characteristics that make them vulnerable to terrorist attacks or for use as shipping conduits by terrorists. These characteristics pertain to both their physical layout and their function. For example:

- Many ports are extensive in size and accessible by water and land. Their accessibility makes it difficult to apply the kinds of security measures that, for example, can be more readily applied at airports.
- Most ports are located in or near major metropolitan areas; their activities, functions, and facilities, such as petroleum tank farms and other potentially hazardous material storage facilities, are often intertwined with the infrastructure of urban life, such as roads, bridges, and factories.
- The sheer amount of material being transported through ports provides a ready avenue for the introduction of many different types of threats.
- The combination of many different transportation modes (e.g., rail and roads) and the concentration of passengers, high-value cargo, and hazardous materials make ports potential targets.

The Port of Tampa illustrates many of these vulnerability characteristics. The port is large and sprawling, with port-owned facilities interspersed among private facilities along the waterfront, increasing the difficulty of access control. It is Florida's busiest port in terms of raw tonnage of cargo, and the cargoes themselves include about half of Florida's volume of hazardous materials, such as anhydrous ammonia, liquid petroleum gas, and sulfur. The port's varied business—bulk freighters and tankers, container ships, cruise ships, fishing vessels, and ship repair and servicing—brings many people onto the port to work daily. For example, in orange juice traffic alone, as many as 2,000 truck drivers might be involved in off loading ships.

The Tampa port's proximity to substantial numbers of people and facilities is another reason for concern. It is located close to downtown Tampa's economic core, making attacks on hazardous materials facilities potentially of greater consequence than for more isolated ports. A number

of busy public roads pass through the port. In addition, located nearby are facilities such as McDill Air Force Base[5] (the location of the U.S. Central Command, which is leading the fighting in Afghanistan) and the Crystal River nuclear power plant, both of which could draw the attention of terrorists.

## Extensive Initiatives Taken by Stakeholders to Address Port Security Since September 11

Since September 11, the various stakeholders involved in ports have undertaken extensive initiatives to begin strengthening their security against potential terrorist threats. As might be expected given the national security aspects of the September 11 attacks, these activities have been most extensive at the federal level. However, states, port authorities, local agencies, and private companies have also been involved. The efforts extend across a broad spectrum of ports and port activities, but the levels of effort vary from location to location.

### Key Federal Agencies Have Taken Important Steps

While many federal agencies are involved in aspects of port security, three play roles that are particularly key—the Coast Guard, Customs Service, and INS.[6] The Coast Guard, which has overall federal responsibility for many aspects of port security, has been particularly active. After September 11, the Coast Guard responded by refocusing its efforts and repositioning vessels, aircraft, and personnel not only to provide security, but also to increase visibility in key maritime locations. Some of its important actions included the following:

- **Conducting initial risk assessments of ports**. These limited risk assessments, done by Coast Guard marine safety personnel at individual ports, identified high-risk infrastructure and facilities within specific areas

[5] We recently reviewed DOD's security programs designed to protect service members and facilities. The review concentrated mostly on the physical security and related aspects of force protection that include measures to protect personnel and property. See General Accounting Office, *Combating Terrorism: Preliminary Observations on Weaknesses in Force Protection for DOD Deployments Through Domestic Seaports*, GAO-02-955T (Washington, D.C.: July 23, 2002).

[6] The federal role extends beyond these three agencies to include agencies and offices in 10 departments (Transportation, Treasury, Justice, Defense, Agriculture, Health and Human Services, Interior, Commerce, Labor, and State), as well as 6 other agencies (Federal Maritime Commission, National Security Council, Central Intelligence Agency, Office of National Drug Control Policy, Environmental Protection Agency, and the Office of the U.S. Trade Representative).

of operation.[7] The assessments helped determine how the Coast Guard's small boats would be used for harbor security patrols. The Port of Tampa received one of these assessments, and the Coast Guard increased the frequency of harbor patrols in Tampa.

- **Redeploying assets**. The Coast Guard recalled all cutters that were conducting offshore law enforcement patrols for drug, immigration, and fisheries enforcement and repositioned them at entrances to such ports as Boston, Los Angeles, Miami, New York, and San Francisco. Many of these cutters are now being returned to other missions, although some continue to be involved in security-related activities.
- **Strengthening surveillance of passenger-related operations and other high-interest vessels**. The Coast Guard established new guidelines[8] for developing security plans and implementing security measures for passenger vessels and passenger terminals, including access controls to passenger terminals and security zones around passenger ships. In Tampa and elsewhere, the Coast Guard established security zones around moored cruise ships and other high-interest vessels, such as naval vessels and tank ships carrying liquefied petroleum gas. The Coast Guard also boarded or escorted many of those vessels to ensure their safe entry into the ports. In some areas, such as San Francisco Bay, the Coast Guard also established waterside security zones adjacent to large airports located near the water.
- **Laying the groundwork for more comprehensive security planning**. The Coast Guard began a process for comprehensively assessing the security conditions of 55 U.S. ports over a 3-year period. The agency has a contract with a private firm, TRW Systems, to conduct detailed vulnerability assessments of these ports. The first four assessments are expected to begin in mid-August 2002, following initial work to develop a methodology and identify security standards and best practices that can be used for evaluating the security environment of ports. Tampa is expected to be among the first eight ports assessed under this process.
- **Driving Maritime Security Worldwide**. The Coast Guard is working through the International Maritime Organization to improve maritime security worldwide. It has proposed accelerated implementation of

[7] Examples of high-risk infrastructure include fossil fuel processing and storage facilities, nuclear power plants, liquid natural gas transfer facilities, naval ships and facilities, and cruise ships and terminal facilities.

[8] The guidelines were contained in a *Navigation and Vessel Inspection Circular*, an approach the Coast Guard uses to provide detailed guidance about enforcement or compliance with certain federal marine safety regulations and Coast Guard marine safety programs.

electronic ship identification systems, ship and port facility security plans, and the undertaking of port security assessments. The proposals have been approved in a security-working group and will be before the entire organization in December 2002.

According to the U.S. Customs Service, it has several initiatives under way in the United States and elsewhere to help ensure the security of cargo entering through U.S. ports. These initiatives include the following:

- **Inspecting containers and other cargoes**. Beginning in the summer of 2002, Customs plans to deploy 20 new mobile gamma ray imaging devices at U.S. ports to help inspectors examine the contents of cargo containers and vehicles. Customs is also adapting its computer-based system for targeting containers for inspection. The system, originally designed for the agency's counter-narcotics efforts, flags suspect shipments for inspection on the basis of an analysis of shipping, intelligence, and law enforcement data, which are also checked against criteria derived from inspectors expertise. These new efforts would adjust the system to better target terrorist threats as well.
- **Prescreening cargo**. In its efforts to increase security, Customs has entered into an agreement to station inspectors at three Canadian ports to prescreen cargo bound for the United States. The agency has since reached similar agreements with the Netherlands, Belgium, and France to place U.S. inspectors at key ports and initiated similar negotiations with other foreign governments in Europe and Asia.
- **Working with the global trade community**. Customs is also engaging the trade community in a partnership program to protect U.S. borders and international commerce from acts of terrorism. In this recent initiative, U.S. importers—and ultimately carriers and other businesses—enter into voluntary agreements with Customs to enhance the security of their global supply chains and those of their business partners. In return, Customs will agree to expedite the clearance of the members' cargo at U.S. ports of entry.

INS is also working on a number of efforts to increase border security to prevent terrorists or other undesirable aliens from entering the United States. INS proposes to spend nearly $3 billion on border enforcement in fiscal year 2003—about 75 percent of its total enforcement budget of $4.1 billion. A substantial number of INS's actions relate to creating an entry and exit system to identify persons posing security threats. INS is working on a system to create records for aliens arriving in the United States and match them with those aliens' departure records. The Immigration and Naturalization Service Data Management Improvement Act of 2000

requires the U.S. Attorney General to implement such a system at airports and seaports by the end of 2003, at the 50 land border ports with the greatest numbers of arriving and departing aliens by the end of 2004, and at all ports by the end of 2005. The USA Patriot Act,[9] passed in October 2001, further instructs the U.S. Attorney General and the Secretary of State to focus on two new elements in designing this system—tamper-resistant documents that are machine-readable at ports of entry and the use of biometric technology, such as fingerprint and retinal scanning. Another Act[10] passed by Congress goes further by making the use of biometrics a requirement in the new entry and exit system.

A potentially more active agency in the future is the new TSA, which has been directed to protect all transportation systems and establish needed standards.[11] To date, however, TSA has had limited involvement in certain aspects of improving port security. TSA officials report that they are working with the Coast Guard, Customs, and other public and private stakeholders to enhance all aspects of maritime security, such as developing security standards, developing and promulgating regulations to implement the standards, and monitoring the execution of the regulations. TSA, along with the Maritime Administration and the Coast Guard is administering the federal grant program to enhance port security. TSA officials also report that they plan to establish a credentialing system for transportation workers.

[9] The USA Patriot Act (P.L. 107-56), signed by the President on October 26, 2001, has various provisions requiring development of technology standards to confirm identity. Under the Act, the Department of Commerce's National Institute of Standards and Technology is to develop and certify accuracy standards for biometric technologies.

[10] The Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173), signed by the President on May 14, 2002, requires that all travel and entry documents (including visas) issued by the United States to aliens be machine-readable and tamper-resistant and include standard biometric identifiers by October 26, 2004.

[11] The Aviation and Transportation Security Act of 2001 (P.L. 107-71) established the TSA under the Secretary of Transportation. The mission of TSA is to protect the nation's transportation systems to ensure freedom of movement for people and commerce by establishing standards for transportation security in collaboration with other federal agencies.

## President and the Congress Have Taken Many Actions and Are Considering Others

The Congress is currently considering additional legislation to further enhance seaport security. Federal port security legislation is expected to emerge from conference committee as members reconcile S. 1214[12] and H.R. 3983.[13] Key provisions of these two bills include requiring vulnerability assessments at major U.S. seaports and developing comprehensive security plans for all waterfront facilities. Other provisions in one or both bills include establishing local port security committees, assessing antiterrorism measures at foreign ports, conducting antiterrorism drills, improving training for maritime security professionals, making federal grants for security infrastructure improvements, preparing a national maritime transportation security plan, credentialing transportation workers, and controlling access to sensitive areas at ports. The Coast Guard and other agencies have already started work on some of the provisions of the bills in anticipation of possible enactment.

Some funding has already been made available for enhanced port security. As part of an earlier DOD supplemental budget appropriation for fiscal year 2002,[14] the Congress appropriated $93.3 million to TSA for port security grants. Three DOT agencies—the Maritime Administration, the Coast Guard, and TSA— screened grant applications and recently awarded grants to 51 U.S. ports for security enhancements and assessments. Tampa received $3.5 million to (1) improve access control, which Tampa Port Authority officials believe will substantially eliminate access to the port by unauthorized persons or criminal elements and (2) install camera surveillance to enforce security measures and to detect intrusions. More recently, Congress passed legislation authorizing an additional $125 million for port security grants, including $20 million for port incident training and exercises.

[12] S. 1214, a bill introduced by Senator Ernest F. Hollings aimed at amending the Merchant Marine Act of 1936 to establish a program to ensure greater security for U.S. seaports, passed in the Senate on December 20, 2001.

[13] H.R. 3983, a bill introduced by Representative Don Young to ensure the security of maritime transportation in the United States against acts of terrorism, passed in the House of Representatives on June 4, 2002.

[14] Department of Defense and Emergency Appropriations for Recovery from and Response to Terrorist Attacks on the United States Act 2002 (Public Law 107-117, H.R. Conference Report 107-350).

## State, Local, and Private Actions Have Varied

The federal government has jurisdiction over navigable waters (including harbors) and interstate and foreign commerce and is leading the way for the nation's ongoing response to terrorism; however, state and local governments are the main regulators of seaports. Private sector terminal operators, shipping companies, labor unions, and other commercial maritime interests all have a stake in port security. Our discussions with public and private sector officials in several ports indicates that although many actions have been taken to enhance security, there is little uniformity in actions taken thus far.

Florida has been a leader in state initiated actions to enhance port security. In 2001—and prior to September 11—Florida became the first state to establish security standards for ports under its jurisdiction and to require these ports to maintain approved security plans that comply with these standards. According to Florida state officials, other states have considered similar legislation. However, according to an American Association of Port Authorities official, Florida is the only state thus far to enact such standards.

Although other states have not created formal requirements as Florida has done, there is evidence that many ports have taken various actions on their own to address security concerns in the wake of September 11. State and local port administrators we spoke with at such locations as the South Carolina State Ports Authority and the Port Authority of New York and New Jersey, for example, said they had conducted security assessments of their ports and made some improvements to their perimeter security and access control. At the eight ports where our work has been concentrated thus far, officials reported expending a total of more than $20 million to enhance security since September 11. Likewise, private companies said they have taken some actions, although they have varied from location to location. For example, one shipping company official said that it had performed a security assessment of its own facility; another facility operator indicated that it had assessed its own security needs and added access controls and perimeter security. In addition, private sector officials at the port of Charleston, South Carolina, told us that some facility operators had done more than others to improve their security. The Coast Guard's Captain of the Port in Charleston agreed with their assessment. He said that one petroleum company has tight security, including access control with a sign-in at the gate and visitor's badge and identification checks for everyone entering the facility. Another petroleum facility requires all visitors to watch a safety and security video, while a third petroleum facility had done so little that the Captain characterized security there as inadequate.

## Challenges Remain in Implementing Standards, Securing Resources, and Building Effective Partnerships

Several challenges need to be addressed to translate the above initiatives into the kind of enhanced security system that the Congress and other policymakers have envisioned. A significant organizational change appears likely to occur with congressional action to establish a new Department of Homeland Security (DHS), which will integrate many of the federal entities involved in protecting the nation's borders and ports. The Comptroller General has recently testified[15] that we believe there is likely to be considerable benefit over time from restructuring some of the homeland security functions, including reducing risk and improving the economy, efficiency, and effectiveness of these consolidated agencies and programs. Despite the hopeful promise of this significant initiative, the underlying challenges of successfully implementing measures to improve the security of the nation's ports remain. These challenges include implementation of a set of standards that define what safeguards a port should have in place, uncertainty about the amount and sources of funds needed to adequately address identified needs, and difficulties in establishing effective coordination among the many public and private entities that have a stake in port security.[16]

### Implementing National Security Standards Could Prove Difficult

One major challenge involves developing a complete set of standards for the level of security that needs to be present in the nation's ports. Adequate standards, consistently applied, are important because lax security at even a handful of ports could make them attractive targets for terrorists interested in smuggling dangerous cargo, damaging port infrastructure, or otherwise disrupting the flow of goods.

In the past, the level of security has largely been a local issue, and practices have varied greatly. For example, at one port we visited most port facilities were completely open, with few fences and many open gates. In contrast, another port had completely sealed all entrances to the

[15] U.S. General Accounting Office, *Homeland Security: Critical Design and Implementation Issues*, GAO-02-957T (Washington, D.C.: July 17, 2002).

[16] Furthermore, GAO is separately conducting reviews related to Customs' processing of sea borne containerized and bulk cargo bound for the United States, focusing on targeting and the use of screening technology. On the basis of our preliminary work at two major U.S. seaports, GAO has identified a number of challenges related to the implementation and effectiveness of Customs' initiatives to ensure the security of cargo entering U.S. seaports. We are unable to further discuss these observations today during this open hearing because of the law-enforcement-sensitive nature of the information. In addition, GAO has ongoing evaluations of INS's efforts to control entry of terrorists into the U.S.

port, and everyone attempting to gain access to port property had to show identification and state their port business before access to the port was granted. Practices also vary greatly among facilities at a single port. At Tampa, for example, a set of state standards applies to petroleum and anhydrous ammonia tanks on port property; but security levels at similar facilities on private land are left to the discretion of private companies.

Development of a set of national standards that would apply to all ports and all public and private facilities is well under way. In preparing to assess security conditions at 55 U.S. ports, the Coast Guard's contractor has been developing a set of standards since May 2002. The Coast Guard standards being developed cover such things as preventing unauthorized persons from accessing sensitive areas, detecting and intercepting intrusions, checking backgrounds of those whose jobs require access to port facilities, and screening travelers and other visitors to port facilities. These standards are performance-based, in that they describe the desired outcome and leave the ports considerable discretion about how to accomplish the task. For example, the standards call for all employees and passengers to be screened for dangerous items or contraband but do not specify the method that must be used for these screenings. The Coast Guard believes that using performance standards will provide ports with the needed flexibility to deal with varying conditions and situations in each location rather than requiring a "cookie-cutter" approach that may not be as effective in some locations as it would be in others.

Developing and gaining overall acceptance of these standards is difficult enough, but implementing them seems likely to be far tougher. Implementation includes resolving thorny situations in which security concerns may collide with economic or other goals. Again, Tampa offers a good example. Some of the port's major employers consist of ship repair companies that hire hundreds of workers for short-term projects as the need arises. Historically, according to port authority officials, these workers have included persons with criminal records. However, new state requirements for background checks, as part of issuing credentials, could deny such persons needed access to restricted areas of the port. From a security standpoint, excluding such persons may be advisable; but from an economic standpoint, a company may have difficulty filling jobs if it cannot include such persons in the labor pool. Around the country, ports will face many such issues, ranging from these credentialing questions to deciding where employees and visitors can park their cars. To the degree that some stakeholders believe that the security actions are unnecessary or conflict with other goals and interests, achieving consensus about what to do will be difficult.

Another reason that implementation poses a challenge is that there is little precedent for how to enforce the standards. The Coast Guard believes it has authority under current law and regulations[17] to require security upgrades, at both public and private facilities. Coast Guard officials have also told us that they may write regulations to address the weaknesses found during the ongoing vulnerability assessment process. However, the size, complexity, and diversity of port operations do not lend themselves to an enforcement approach such as the one the United States adopted for airports in the wake of September 11, when airports were shut down temporarily until they could demonstrate compliance with a new set of security procedures. In the case of ports, compliance could take much longer, require greater compromises on the part of stakeholders, and raise immediate issues about how compliance will be paid for—and who will bear the costs.

## Funding Issues Are Pivotal

Many of the planned security improvements at seaports will require costly outlays for infrastructure, technology, and personnel. Even before September 11, the Interagency Commission on Crime and Security in U.S. Seaports[18] estimated the costs for upgrading security infrastructure at U.S. ports ranging from $10 million to $50 million per port.[19] Officials at the Port of Tampa estimated their cost for bringing the port's security into compliance with state standards at $17 million—with an additional $5 million each year for security personnel and other recurring costs.

Deciding how to pay for these additional outlays carries its own set of challenges. Because security at the ports is a concern shared among federal, state, and local governments, as well as among private commercial interests, the issue of who should pay to finance antiterrorism activities may be difficult to resolve. Given the importance of seaports to our nation's economic infrastructure and the importance of preventing dangerous persons or goods from entering our borders, it has been argued by some that protective measures for ports should be financed at the

[17] Ports and Waterways Safety Act, 33 U.S.C. section 1226; and Title 33 (Navigation and Navigable Waters) Code of Federal Regulations, part 6 (Protection and Security of Vessels, Harbors, and Waterfront Facilities).

[18] On April 27, 1999, the President established the Interagency Commission on Crime and Security in U.S. Seaports. The Commission issued its report on August 28, 2000.

[19] Estimated range varies on the basis of port size and cost of the technology component of the security upgrade.

federal level. Port and private sector officials we spoke with said that federal crime, including terrorism, is the federal government's responsibility, and if security is needed, the federal government should provide it. On the other hand, many of the economic development benefits that ports bring, such as employment and tax revenue, remain within the state or the local area. In addition, commercial interests and other private users of ports could directly benefit from security measures because steps designed to thwart terrorists could also prevent others from stealing goods or causing other kinds of economic damage.

The federal government has already stepped in with additional funding, but demand has far outstripped the additional amounts made available. For example, when the Congress appropriated $93.3 million to help ports with their security needs, the grant applications received by TSA totaled $697 million—many multiples of the amount available (even including the additional $125 million just appropriated for port security needs). However, it is not clear that $697 million is an accurate estimate of the need because, according to the Coast Guard and Maritime Administration officials, applications from private industry may have been limited because of the brief application period. In Tampa, while officials believe that they need $17 million for security upgrades, they submitted an application for about $8 million in federal funds and received $3.5 million.

In the current environment, ports may have to try to tap multiple sources of funding. Tampa officials told us that they plan to use funds from a variety of state, local, and federal sources to finance their required security improvements. These include such sources as federal grants, state transportation funds, local tax and bond revenues, and operating revenues from port tenants. In Florida, one major source for security money has been the diversion of state funds formerly earmarked for economic development projects. According to Florida officials, in 2002, for example, Florida ports have spent virtually all of the $30 million provided by the state for economic development on security-related projects. Ports throughout the nation may have varying abilities to tap similar sources of funding. In South Carolina, for example, where port officials identified $12.2 million in needed enhancements and received $1.9 million in TSA

grants, officials said no state funding was available.[20] By contrast, nearby ports in North Carolina, Georgia, and Virginia do have access to at least some state-subsidized funding. South Carolina port officials also reported that they had financed $755,000 in security upgrades with operating revenue, such as earnings from shippers' rental of port-owned equipment, but they said operating revenues were insufficient to pay for much of the needed improvements.

These budget demands place pressure on the federal government to make the best decisions about how to use the funding it makes available. Governments also have a variety of policy tools, including grants, regulations, tax incentives, and information-sharing mechanisms to motivate or mandate other lower levels of government or the private sector to help address security concerns, each with different advantages or drawbacks, for example, in achieving results or promoting accountability. Security legislation currently under consideration by the Congress includes, for example, federal loan guarantees as another funding approach in addition to direct grants.

## Shared Responsibilities Place a Premium on Effective Communication and Coordination

Finally, once adequate security measures are in place, there are still formidable challenges to making them work. As we have reported, one challenge to achieving national preparedness and response goals hinges on the federal government's ability to form effective partnerships among many entities.[21] If such partnerships are not in place—and equally important, if they do not work effectively—those who are ultimately in charge cannot gain the resources, expertise, and cooperation of the people who must implement security measures. One purpose in creating the proposed DHS is to enhance such partnerships at the federal level.

[20] According to a port authority official, by their charter, South Carolina's ports are structured for self-sufficient operation and do not receive any state funds. Other fiscal constraints identified by South Carolina port officials include their inability to divert funds to security needs from nonsecurity-related improvement projects, because those projects are included in contracts with the ports' customers. Also, state law allows the State Ports Authority to borrow money, but only if it is for a revenue-generating project, such as a container crane. Furthermore, State Ports Authority officials have considered levying a security surcharge from their customers. However, they concluded that it would place their ports at a competitive disadvantage unless other ports also instituted a surcharge.

[21] U.S. General Accounting Office, *Homeland Security: Intergovernmental Coordination and Partnership Will Be Critical to Success*, GAO-02-899T (Washington D.C.: July 1, 2002), GAO-02-900T (Washington, D.C.: July 2, 2002), and GAO-02-901T (Washington, D.C.: July 3, 2002).

Part of this challenge involves making certain that all the right people are involved. At the ports we reviewed, the extent to which this had been done varied. The primary means of coordination at many ports are port security committees, which are led by the Coast Guard; the committees offer a promising forum for federal, state, and local government and private stakeholders to share information and make decisions collaboratively. For example, a Captain of the Port told us that coordination and cooperation among port stakeholders at a port in his area of responsibility are excellent and that monthly meetings are held with representation from law enforcement, the port authority, shipping lines, shipping agents, and the maritime business community. However, in another port, officials told us that their port security committees did not always include representatives from port stakeholders who were able to speak for and make decisions on behalf of their organization.

An incident that occurred shortly before our review at the Port of Honolulu illustrates the importance of ensuring that security measures are carried out and that they produce the desired results. The Port had a security plan that called for notifying the Coast Guard and local law enforcement authorities about serious incidents. One such incident took place in April 2002, when, as cargo was being loaded onto a cruise ship, specially trained dogs reacted to possible explosives in one of the loads, and the identified pallet was set aside. Despite the notification policy, personnel working for the shipping agent and the private company providing security at the dock failed to notify either local law enforcement officials or the Coast Guard about the incident. A few hours after the incident took place, Coast Guard personnel conducting a foot patrol found the pallet and inquired about it, and, when told about the dogs' reaction, they immediately notified local emergency response agencies. Once again, however, the procedure was less than successful because the various organizations were all using radios that operated on different frequencies, making coordination between agencies much more difficult.

Fortunately, the Honolulu incident did not result in any injuries or loss, and Coast Guard officials said that it illustrates the importance of practice and testing of security measures. They also said that for procedures to be effective when needed they must be practiced and the exercises critiqued so the procedures become refined and second nature to all parties. According to a Coast Guard official, since the April incident, another incident occurred where another possible explosive was detected. This time all the proper procedures were followed and all the necessary parties were contacted.

One aspect of coordination and cooperation that was lacking in the standard security measures we observed is the sharing of key intelligence about such issues as threats and law enforcement actions. No standard protocol exists for such an information exchange between the federal government and the state and local agencies that need to react to it. In addition, no formal mechanism exists at the ports we visited for the coordination of threat information. State and local officials told us that for their governments to act as partners with the federal government in homeland security, of which port security is a critical part, they need better access to threat information.

We identified a broad range of barriers that must be overcome to meet this challenge. For example, one barrier involves security clearances. Officials at the National Emergency Management Association (NEMA), the organization that represents state and local emergency management personnel, told us that personnel in the agencies they represent have difficulty in obtaining critical intelligence information. Although state or local officials may hold security clearances issued by the Federal Emergency Management Agency, other federal agencies, such as the Federal Bureau of Investigation, do not generally recognize these security clearances. Similarly, officials from the National Governors Association told us that because most state governors do not have a security clearance, they cannot receive any classified threat information. This could affect their ability to effectively use the National Guard or state police to prevent and respond to a terrorist attack, as well as hamper their emergency preparedness capability.[22]

The importance of information-sharing on an ongoing basis can be seen in an example of how discussions among three agencies, each with its own piece of the puzzle, first failed but then uncovered a scheme under which port operations were being used to illegally obtain visas to enter the United States. The scheme, which was conducted in Haiti, was discovered only after a number of persons entered the United States illegally. Under this scheme, people would apply at the U.S. Consulate in Haiti for entrance visas on the pretext that they had been hired to work on ships that were about to call at the Port of Miami. However, the ships were no longer in service. The Coast Guard knew that these ships were no longer in service, but this information was not known by the State Department (which

[22] U.S. General Accounting Office, *Homeland Security: Progress Made; More Direction and Partnership Sought*, GAO-02-490T (Washington, D.C.: March 12, 2002).

issued the visas) or INS (which admitted the people into the United States). A Coast Guard official at the Miami Marine Safety Office estimated that hundreds of people entered the country illegally in 2002.[23] Once this was discovered by Coast Guard personnel, they contacted certain American embassies to inform them of the vessels that have been taken out of active service or have been lost at sea and instituted procedures to ensure that the potential crew member was joining a legitimate vessel.

The breadth of the challenge of improved coordination and collaboration is evident in the sheer magnitude of the players, even if the proposed DHS is enacted. Coordination challenges will remain among the 22 federal entities that would be brought together in the proposed DHS; between these diverse elements of DHS and the many entities with homeland security functions still outside DHS; and between the full range of federal entities and the myriad of state, local, and private stakeholders.

In summary, Mr. Chairman, making America's ports more secure is not a short-term or easy project. There are many challenges that must be overcome. The ports we visited and the responsible federal, state, and local entities have made a good start, but they have a long way to go. While there is widespread support for making the nation safe from terrorism, ports are likely to epitomize a continuing tension between the desire for safety and security and the need for expeditious, open flow of goods both into and out of the country.

This completes my prepared statement. I would be pleased to respond to any questions you or other Members of the Subcommittee may have.

## Contacts and Acknowledgments

For information about this testimony, please contact JayEtta Z. Hecker, Director, Physical Infrastructure Issues, on (202) 512-2834. Individuals making key contributions to this testimony included Randy Williamson, Steven Calvo, Jonathan Bachman, Jeff Rueckhaus, and Stan Stenersen.

[23] The Coast Guard official developed the estimate after one of the leaders who was selling the fraudulent documents was arrested in Miami.

# Appendix: Scope and Methodology

To learn of the vulnerabilities present at ports, the initiatives undertaken since September 11 to mitigate them and the challenges that could impede further progress, we judgmentally selected 10 ports—8 of which we visited—to provide a geographically diverse sample and, in many cases, include ports where special attention had been devoted to security issues. For example, we visited the ports in Tampa, Miami, and Ft. Lauderdale (Port Everglades) because they—like all of Florida's deepwater ports—are required to implement state-mandated security standards, and because they handle large numbers of cruise passengers or large quantities of containerized or bulk cargoes. While in Florida, we also met with state officials from the Office of Drug Control, which developed the port security standards and the legislation codifying them, and from the Department of Law Enforcement, charged with overseeing the implementation of the state standards. In addition, we visited ports in Charleston, South Carolina, and Honolulu, Hawaii, which had been the subject of detailed vulnerability studies by the Defense Threat Reduction Agency (DTRA), in order to determine their progress in implementing the security enhancements recommended by DTRA. For further geographical representation we visited the ports in Oakland, California; Tacoma, Washington; and Boston, Massachusetts, and held telephone discussions with officials from the Port Authority of New York and New Jersey and with the Coast Guard in Guam. At each port visit, we toured the port on land and from the water in order to view the enhancements made since September 11 and the outstanding security needs. We also interviewed officials from the Coast Guard and other public and private sector port stakeholders, such as port authorities, state transportation departments, marine shipping companies, shipping agents, marine pilots, and private terminal operators.

To determine federal, state, local, and private initiatives to enhance port security and the implementation challenges, we had several conversations with officials from the Coast Guard headquarters, DTRA, the Maritime Administration, the American Association of Port Authorities, and the private contractor recently hired by the Coast Guard to conduct comprehensive vulnerability assessments at 55 U.S. ports. These discussions included issues related to port security assessments—both completed and planned—communication and coordination with port stakeholders, federal funding of port security enhancements, and other issues. In addition, we analyzed administrative data from the federally funded TSA Port Security Grant Program for additional information on the security needs of ports and the ports' progress since September 11 in enhancing their security.

# Related GAO Products

## Homeland Security

*Homeland Security: Critical Design and Implementation Issues* (GAO-02-957T, July 17, 2002)

*Homeland Security: Title III of the Homeland Security Act of 2002* (GAO-02-927T, July 9, 2002)

*Homeland Security: Intergovernmental Coordination and Partnerships Will Be Critical to Success* (GAO-02-899T, July 1, 2002).

*Homeland Security: New Department Could Improve Coordination but May Complicate Priority Setting* (GAO-02-893T, June 28, 2002).

*Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Will be Pivotal to Success* (GAO-02-886T, June 25, 2002).

*Homeland Security: Key Elements to Unify Efforts Are Underway but Uncertainty Remains* (GAO-02-610, June 7, 2002).

*National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy* (GAO-02-811T, June 7, 2002).

*Homeland Security: Responsibility And Accountability For Achieving National Goals* (GAO-02-627T, April 11, 2002).

*National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts Is Critical to an Effective National Strategy for Homeland Security* (GAO-02-621T, April 11, 2002).

*Homeland Security: Progress Made; More Direction and Partnership Sought* (GAO-02-490T, March 12, 2002).

*Homeland Security: Challenges and Strategies in Addressing Short- and Long-Term National Needs* (GAO-02-160T, November 7, 2001).

*Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts* (GAO-02-208T, October 31, 2001).

*Homeland Security: Key Elements of a Risk Management Approach* (GAO-02-150T, October 12, 2001).

*Homeland Security: A Framework for Addressing the Nation's Issues* (GAO-01-1158T, September 21, 2001).

## Combating Terrorism

*Combating Terrorism: Preliminary Observations on Weaknesses in Force Protection for DOD Deployments Through Domestic Seaports* (GAO-02-955T, July 23, 2002).

*Combating Terrorism: Intergovernmental Cooperation in the Development of a National Strategy to Enhance State and Local Preparedness* (GAO-02-550T, April 2, 2002).

*Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy* (GAO-02-549T, March 28, 2002).

*Combating Terrorism: Critical Components of a National Strategy to Enhance State and Local Preparedness* (GAO-02-548T, March 25, 2002).

*Combating Terrorism: Intergovernmental Partnership in a National Strategy to Enhance State and Local Preparedness* (GAO-02-547T, March 22, 2002).

*Combating Terrorism: Key Aspects of a National Strategy to Enhance State and Local Preparedness* (GAO-02-473T, March 1, 2002).

*Combating Terrorism: Considerations For Investing Resources in Chemical and Biological Preparedness* (GAO-01-162T, October 17, 2001).

*Combating Terrorism: Selected Challenges and Related Recommendations* (GAO-01-822, September 20, 2001).

*Combating Terrorism: Actions Needed to Improve DOD's Antiterrorism Program Implementation and Management* (GAO-01-909, September 19, 2001).