Protecting America's Ports: Promising Practices

A Final Report
Submitted by the
Police Executive Research Forum
to the
National Institute of Justice

Antony Pate
Bruce Taylor
Bruce Kubu

November 20, 2007

Acknowledgments

Our acknowledgments must begin with Dr. Rexford B. Sherman, Director of Research and Information Services at the American Association of Port Authorities (AAPA), with whom we established an extremely productive relationship early on in this project. Rex became our greatest resource, sharing his expertise on the nature of the maritime industry and the roles of the various actors involved in port security. He also helped us formulate the particular questions we would attempt to answer in this report. Rex provided access to decision makers at critical ports, and helped us to make introductory visits. He also helped us identify and recruit members of our advisory board. Throughout the project, Rex has been there when we needed him, giving us advice, providing us access, and inviting us to AAPA port security meetings. Thank you Rex. This report would not have been possible without your assistance.

Rex also introduced us to the members of the Security Committee of the AAPA, a group of security professionals responsible for protecting our nation's ports. As it turned out, this "introduction" was akin to having your father "introduce" you to swimming by throwing you off the pier. We were asked by the chairman of the committee, Captain Ralph Tracy of the Port of Los Angeles Port Police, to explain the goals and expected products of our work. If the committee agreed to cooperate with our effort, they would lend their support. If they did not agree, we would be on our own. The lack of support, we recognized, would amount to a sea change in our voyage,--the difference between a successful launch and a sunken vessel. After making our pitch, we were told to leave the room while the committee deliberated. Fortunately, the committee agreed to support our effort. From that moment on, the Security Committee, and the AAPA, gave unstinting assistance to our work. Committee members answered our questions, gave us advice, provided contacts, and in every conceivable way made it possible to conduct this difficult project. We express our inestimable gratitude to Captain Ralph Tracy of the Los Angeles Port Police and all of the other members of the Security Committee for their assistance.

Armed with advice from the Security Committee, our readings, our attendance at port security conferences, and the insights gleaned during familiarity visits to the ports of Baltimore, Miami, San Diego, Los Angeles, and Long Beach, we began to assemble a project advisory board. We tried to "cover the waterfront," representing the broad range of stakeholders in the port security community. We relied on this group in reviewing our research plan, critiquing our site visit protocol, suggesting sites to be visited, and assisting us in setting up site visits. Because they came to our rescue in countless ways, we acknowledge our profound gratitude to all of them. The group, in alphabetical order, consisted of:

- Edward Badolado, Executive Vice President of Homeland Security, Shaw Group[1];
- Charles (Chuck) Carroll, Jr., Executive Director, National Association of Waterfront Employers;
- Carlos Cortez, Immigration and Customs Enforcement, Department of Homeland Security;
- Stan Deno, Security Director, International Council of Cruise Lines;

[1] Now President of Integrated Infrastructure Analytics, Inc.

- Paul Hankins, Transportation Security Administration, Department of Homeland Security;
- Betty Kelepecz; Chief of Police, San Diego Harbor Police[2];
- Joe Lawless, Public Safety Director, Massachusetts Port Authority;
- George Lerner, Chief of Police, Port of Stockton;
- Timothy Mann, Captain, Supervisor, Port Security Assessment Team, U.S. Coast Guard;
- Bruce Marquis, Chief of Police, Norfolk, Virginia;
- R. Douglas Rhoads, Vice President, Operations; Manuel, Daniels, Burke International;
- Todd Ripley, U.S. Maritime Administration;
- Robert Rowe, Director of Development, ASIS International;
- Martin Rojas, Executive Director, American Trucking Associations;
- Ted Thompson, Executive Vice President, International Council of Cruise Lines;
- Mike Toddington, Executive Director, International Association of Airport and Seaport Police;
- Bill Wanamaker, Director, American Trucking Associations; and
- Barry Wilkins, Managing Director, National Cargo Security Committee.

We owe particular thanks to Captain Mann of the U.S. Coast Guard, who served as our liaison with his agency and made it possible for us to meet with the Captain of the Port in each of the sites we visited.

With the assistance of all of those mentioned above, we made successful site visits to 17 ports: Boston, Charleston, Galveston, Houston, Jacksonville, Long Beach, Los Angeles, Miami, New Orleans, Port Lauderdale, San Diego, Savannah, Seattle, Tacoma, Tampa, Texas City, and Virginia. In each port, we relied on the cooperation and assistance of countless persons. To prevent the Acknowledgments from approaching the length of the report itself, we will simply say that we express our appreciation to all who helped us arrange the visits and our sincere thanks to all who allowed us to interview or accompany them.

Dr. Donald Faggiani, who was Senior Research Associate at PERF at the time this project began, contributed significantly to the start-up efforts involved. Although he has moved on to other endeavors, we extend our appreciation for all the help he provided.

Last, but by no means least, we express our profuse and warm appreciation to our project monitor at the National Institute of Justice, Lois Mock. She got her sea legs along with us on many of our site visits, guided us through difficult and sometimes stormy waters, and had the patience to not jump ship before we completed our assignment.

Antony Pate
Bruce Taylor
Bruce Kubu

[2] Now retired.

Table of Contents

Protecting America's Ports: Promising Practices

Executive Summary

I. Introduction

The massive flow of shipping containers around the world provides the backbone for the world's economy. The global shipping system is a critical infrastructure, but it is very vulnerable. The contents of less than 2 percent of all containers are checked, according to official estimates. Containers have been used by criminals to transport all sorts of banned goods, and even people.

In recent years, the illegal transport of goods and people has become a particularly worrisome problem in light of world terrorism. Terrorists could, for example, use containers to transport dangerous materials or weapons, or they could use the containers themselves as weapons of mass destruction. Prior to the September 11 attacks, these threats were not "front burner" issues for seaport officials. Before September 11, 2001, seaport security agencies focused on general criminal activity and physical security and access control, cargo security, passenger and crew security, and military mobilization security. Although the maritime community acknowledged the threat of terrorism prior to 9/11, very few comprehensive security measures were taken to deter or undermine a maritime terrorist threat.

Nevertheless, a number of *ideas* for improving seaport security had been proposed prior to 9/11, including: developing port security plans, developing new ways to track cargo, "pushing the borders of the nation out," sealing the supply chain by taking steps to ensure that cargoes are controlled and "sealed" at each step of their journeys, designating a lead agency for port security, and using public-private partnerships to carry out security tasks.

In general, these port security efforts lacked urgency. However, after September 11, the U.S. government began to focus on the gravity of the threat, as manifested in the November 2002 Maritime Transportation Security Act (MTSA), a new federal law with dozens of strict new provisions governing the safeguarding of shipping.

Since September 11, the U.S. government has been developing a number of initiatives to safeguard U.S. seaports, including:

- Both short- and long-range vessel detection and monitoring capabilities;
- Initiatives and agreements to improve advance notices of arrival, vessel movement information, supply-chain security practices, and manifest and entry information for cargo;
- International arrangements that promote visibility into the maritime supply chain;
- Sensor technology, intelligence and information processing tools to monitor the maritime;
- International coalitions to share maritime situational awareness on a timely basis;
- Enhanced global maritime intelligence and coordination;
- Shared situational awareness to disseminate information to users at all levels;
- Automated tools to improve data fusion, analysis, and management in order to improve tracking and detection of aberrant patterns of activity; and
- Research in information processing to increase threat detection capabilities.

These federal initiatives have been implemented to varying degrees and have increased security in varying ways in seaports. Local seaports also have implemented additional security enhancements.

II. Methods

Our study attempted to identify the best and most promising local practices in port security. We also explored situations where there were compelling local adaptations of a nationwide practice. Our focus on "best" and "promising" practices is somewhat subjective, necessitated by a general lack of rigorous evaluation work in this area. The existing set of port security practices has not been evaluated, even with non-rigorous methods. Nevertheless, port security officials have had considerable experience with a number of these practices, and our report offers their valuable insights into practices that have been applied in a variety of settings. In general, the port sites were very generous in providing us access to the full range of port activities and security initiatives. Nevertheless, due to the sensitivity of the data we collected and its potential for compromising security at our Nation's ports, we had to limit some of the details we could provide in our descriptions of the local initiatives.

Given the considerable uncertainty around port security operations and the interconnections across the many local, state and federal law enforcement partners involved in providing security, we used an exploratory/descriptive case study methodology. We conducted descriptive case studies of exemplary and innovative security practices in 17 seaports, with a particular focus on intergovernmental and public-private partnerships and elements of success of those partnerships. While various research methods have their strengths and weaknesses, the descriptive case study is the preferred methodology for analyzing the inter-organizational relationships present in port security operations. At the time of this study, ooo little was known about this subject matter to embark on an evaluation of the effects of various port security efforts. This project is a first step. In this project we assemble a rich description of the problem and context for port security and identify key promising practices based on the expert opinion of port personnel. At a later stage, researchers will be in a better position to address some of the questions about the effectiveness of the various security initiatives.

With the assistance of a project advisory board, the research team selected 17 ports to be visited: San Diego, CA; Los Angeles, CA; Long Beach, CA; Jacksonville, FL; Tampa, FL; Ft. Lauderdale, FL; Miami, FL; New Orleans, LA; Houston, TX; Galveston, TX; Texas City, TX; Charleston, SC; Savannah, GA; Port of Virginia, VA; Boston, MA; Seattle, WA; and Tacoma, WA. (The report describes the criteria we used in selecting the sites to be visited.) Members of the site visit team interviewed a wide range of persons involved in managing each port and providing for its security, including:

- Captain of the Port and other U.S. Coast Guard representatives;
- Port Authority Manager/Director;
- Port Security Director;
- Facility Security Officers;
- Port Authority Police Chief (if any) and officers;
- Representatives of local, county, and state police agencies involved with port security;
- Representatives of other federal government agencies involved with port security;
- Representatives from private security agencies, if appropriate;
- Representatives of local fire departments;
- Representatives of tenants in the port, if appropriate;
- Representatives of unions and stevedores; and
- Others, as identified.

At each site, the evaluation team addressed the following issues:

- Port management structure and the primary security concerns in and around the port;
- Use and status of port security plan(s) and identification of the agencies responsible for providing port security;
- Nature of the relationship among the main stakeholders involved in providing security;
- Status and role of Maritime Regional Security Committee (or its equivalent);
- Participation in the local maritime security committee;
- Sources of intelligence with regard to security threats;
- Role of local Joint Terrorism Task Force in port security;
- Status of background checks conducted for personnel working at the port;
- Status of perimeter patrols around the port—landside and seaside;
- Enforcement of access control for entry to the port and separate terminals within the port;
- Status of credentials for persons entering the port;
- Inspection of containers and other cargo coming into and leaving the port;
- Security for public spaces within the port;
- Type and level of training for port security personnel;
- Plans for responding to a terrorist attack and exercises to practice implementing those plans;
- Plans to mediate the effects of a possible attack and roles of various agencies in those plans;
- Plans to restore the port to operational condition following an incident.

III. Results

The section that follows provides a description of what our team (and the experts we consulted) felt were promising practices in port security. The data to compare which were the best among these promising practices were just not available. We believe it would be misleading to offer a prioritized list. Each port will need to consider our results one-by-one and assess their relevance to their port, given their own local conditions and circumstances. We identified promising practices related to improvement in five general areas including:

- *Awareness* of threats to a port
- *Prevention* of attacks on a port
- *Preparedness* for an attack against a port
- *Response* after an attack
- *Recovery* after an attack.

(1) *Awareness:* Across our set of study ports, two main efforts have been undertaken to increase awareness of the potential for attacks against seaports:

- Stakeholder coordination and collaboration initiatives
- Protocols for detecting and monitoring port-related security risks/intelligence sharing.

First, in the area of stakeholder coordination and collaboration initiatives, we observed a range of activities under the Area Maritime Security Committees (AMSC). AMSCs serve as forums for local seaport stakeholders from federal agencies, state and local government, law enforcement, and private industries to gain a comprehensive perspective of security issues at the

nation's seaports. AMSCs are tasked with collaborating on plans to secure their ports so the resources of an area can be best used to raise maritime awareness of terrorism and to deter, prevent and respond to terror threats. The Coast Guard has established committees in all the nation's ports to coordinate the activities of port stakeholders. Although AMSCs existed at all the ports visited by the evaluation team, they vary considerably in terms of their membership size, types of stakeholders represented, frequency of convening, and methods of functioning. AMSCs disseminate information through regularly scheduled meetings, issuance of electronic bulletins on suspicious activities around seaport facilities, and sharing key documents. Many of the AMSCs have been able to integrate the work of many of the existing stakeholder groups, including recruiting members that have security clearances. Some ports have formed similar working groups that are not named Area Maritime Security Committees. For example, the Ports of Seattle and Tacoma are part of the South Puget Sound Port Security Committee (SPSPSC)**.** The SPSPSC helps coordinate planning, information sharing, and other necessary activities to enhance port security.

Second, in addition to the Area Maritime Security Committees, several ports have created other methods by which they can share information and intelligence through protocols for detecting and monitoring port-related security risks and systems for increasing intelligence-sharing. Some of the most promising of these approaches were found in the ports in Boston, Charleston, Houston, Jacksonville, Los Angeles, New Orleans, Port Everglades, San Diego, Savannah, Seattle, Tacoma, Tampa and Texas City. Some of these best practices were port–specific, such as Project Seahawk in Charleston, while others were broader homeland security efforts designed to protect all the vulnerable targets found in a state (e.g., the State Fusion Center in Boston). Some of these efforts were undertaken daily, such as daily security briefings held at the Port of Boston involving local, state, and federal law enforcement, as well as representatives of private industry, to discuss information that might be relevant to security at either the port or Logan airport. Similar daily security briefings are held at the ports in Charleston, Port Everglades, and Tampa (which conducts daily security briefings by e-mail or telephone conferences). These briefings often include discussion of developments in port security, including suspicious activities, outstanding warrants, and recent intelligence. Some of these briefings also involve private security and facility security officers.

The best practices for enhancing awareness that were port-specific include port intelligence teams or special units within homeland security centers. For example, Houston's awareness-building efforts are coordinated by the Coast Guard; Tacoma has a Maritime Intelligence Support Team led by the Port Security Service; and Charleston has Project Seahawk, which has an intelligence unit that builds awareness of threats to the port. These teams or units often collect and analyze intelligence information that may affect port security and reach out to members of the maritime community to inform them of the importance of identifying possible terrorist suspects and the need to convey that information to law enforcement officials. Similar work is also done by the Tampa Port Watch group, which functions like a neighborhood watch for the maritime community. The San Diego Harbor Police Homeland Security Unit coordinates community outreach and public awareness campaigns to make port tenants, marina residents, hospitality workers and others more aware of terrorist activities and how to report them.

Another port-specific best practice in this area involves the managing or structuring of information technology. Charleston's Yard Management System (YMS) is an excellent example of a system that provides a high level of integration between security and operational data. The YMS is an excellent aid for increasing security at the port by allowing the tracking of all cargo into and out of the port and all the equipment used for moving the cargo. Savannah's Navis WebAccess system provides key stakeholders in the port/terminal community with access to pertinent terminal transaction information to address security concerns. Tacoma's Central Point of Coordination Rail Management System links security data with operational data and serves as a safety and security support tool in the event of either a natural disaster or an act of terrorism. Seattle's MPS/ATLAS system provides total supply-chain visibility, with early loss and damage detection and a means of mitigating potential security threats to the port.

Other port-specific security measures for enhancing awareness include a variety of committees and councils, such as the Seattle-Washington State Ferry Security Committee**,** the Texas City Port Security Council, the Los Angeles Port Community Advisory Committee, and the Houston Law Enforcement Subcommittee of the Area Maritime Security Committee of the Port of Houston. Also, port-specific security measures to increase awareness are in place in Charleston, which, in addition to a port police agency, has a voluntary port security force and has the South Carolina Naval Militia comprised of Navy reservists who provide information to authorities concerning suspicious activities. The Port of Houston has some similar volunteer groups in place.

Some of the best practices for raising awareness that were not port-specific but rather were part of a broader homeland security effort include a number of fusion centers that address port security. For example, the Port of Boston works with the Massachusetts State Fusion Center; the Port of Savannah works with the Georgia Fusion Center; the Port of Los Angeles works with its Regional Terrorism Threat Assessment Center and Joint Regional Intelligence Center; and the Port of Houston works with the Texas Security Alert and Analysis Center. Also, a variety of terrorism task forces address port security (Joint Terrorism Task Forces [JTTF] based in Boston, Houston, and Jacksonville; the Jacksonville Northeast Florida Domestic Security Task Force; and the Tampa Regional Florida Domestic Security Task Force), and a number of anti-terrorism councils and groups also address port security (the Houston Anti-Terrorism Advisory Council, the FBI's Counter-Terrorism Intel Group in Houston, the Houston Energy Security Council, the Los Angeles County Terrorism Early Warning Group, the Louisiana Anti-Terrorism Advisory Council, and an Urban Area Security Initiative group based in New Orleans). Also, the Port of San Diego works with its local Terrorism Early Warning (TEW) Group and Regional Information Sharing and Analysis (RISA) project to raise awareness about port security.

(2) *Prevention:* This was the most common category of measures taken to increase port security. Prevention is a critical component of port security, based on the premise that a strong, visible defense will deter or delay an attack.

In the area of preventing attacks against ports, we identified a number of promising practices, including:

- Improvements of physical security/infrastructure at seaports
- Protocols and processes limiting entry to seaports

- Technological detection/inspection systems
- Law enforcement-related activities
- Interagency operational centers

First, in the area of area of physical security there are a number of ways to secure the outer and inner perimeters of a port. Our team observed a number of promising practices in the area of physical security, including perimeter security; fencing, walls and other barricades; security towers and platforms; and lighting. We also learned of the need for minimum standards in the area of physical infrastructure, and the problem of restricting waterside access to port facilities. While there is a need for many high-tech security devices, there is still a need for "low-tech" measures such as fencing. While regular fences can be easily circumvented, a variety of security enhancements can be added to make it more difficult to break through or bypass a fence. Concrete anti-vehicle barricades, caltrops, and spike-strips can also be used with fences if there is a need to stop a motor vehicle. These low-cost, high-value protective features can be used in a myriad of ways to protect sensitive elements in a port. We also observed innovations in seaborne security/ floating booms and barriers in Boston and Port Everglades. In Boston, floating barriers are being used around cruise ships and LNG tankers when they are in port. In Port Everglades, portable floating booms are used around cruise ships when they are docked in the port to protect against seaborne attacks.

Lighting of docks, container traffic, and storage areas is also an important security measure. Some ports make use of mobile light towers and solar-powered emergency street lights. Another simple strategy used by most of the ports we visited was door-to-door stacking of empty shipping containers. While not a foolproof system, stacking containers door-to-door is a very simple method of limiting terrorists, stowaways, thieves or smugglers with contraband from gaining entry into shipping containers.

Second, we observed a number of promising protocols and practices that have been established to limit entry to seaports, including enhanced access control, the use of new-technology detection systems, changes in law enforcement, and the use of interagency operational centers.

Although seaports have historically used conventional forms of access control such as ID badges, there is a movement now to technology-intensive access control systems. The pending emergence of the Transportation Worker Identification Credential (TWIC) will transform access control throughout U.S. seaports. In advance of TWIC, a number of ports have developed local credentialing systems (e.g., the Florida Uniform Port Access Credential Card). Seaports are also turning to other types of access control devices, such as biometric controls based on facial, retina, iris, fingerprint, and hand geometry scans. In addition to high-tech solutions, some ports have instituted some simple low-cost measures to help control access to the port (e.g., worker identification numbers stenciled on port-issued color-coded work clothes, for easy identification of authorized personnel by security workers). Also, some large port facilities are now requiring all personnel working or visiting the facility to travel between facility areas on a facility shuttle bus, thereby limiting access to unauthorized areas. We also learned about a variety of schemes for limiting unauthorized ship access at anchorage.

Third, seaports are deploying numerous high-tech detection systems to secure the complete spectrum of seaport operations and physical assets. These systems have great potential, especially when used in combination with traditional security practices, including CCTV, sensory detection systems, Non-Intrusive Inspection Technology, and vehicle tracking systems. The use of CCTV at seaports is highly prevalent. Seaports are starting to adopt an airport model, in which a single graphical-user interface handles all access-control, CCTV, DVR, and video-analytics requirements from a central head-end location. Also, some of the better systems we observed combine CCTV and video analytics software algorithms to analyze video proactively based upon behavior.

Another promising practice is the use of sensor technologies to serve as cargo screeners. As with many technologies, these sensory devices can be helpful, but there is still no technological substitute for good security procedures and well-trained human inspectors. Also, a major challenge in deploying many of these technologies at a port facility is the communication infrastructure; most ports were never designed to move video and data communications from one side of the facility, harbor or perimeter to the other.

Another terrorism prevention measure at seaports is the use of Non-Intrusive Inspection (NII) technologies to accelerate the screening of container traffic. Gamma ray and X-ray imaging systems are being used to screen conveyances for contraband and WMDs. Radiation Portal Monitors (RPM) provide a passive, non-intrusive means of screening trucks and other conveyances for the presence of nuclear and radiological materials. Density meters and fiber-optic scopes are being used to peer inside suspicious containers. Vehicle and Cargo Inspection Systems (VACIS) are also being used to examine dense freight in order to detect contraband and potentially dangerous goods. Another promising practice is electronic tracking systems installed on trucks transporting containers in and out of the port. However, with many of these systems, protocols for their use are still in development, and the limits of these systems are still being uncovered. Also, ports that implement these type systems may have to overcome employee relations issues about the nature and purpose of these systems.

Fourth, expanded police patrol is another preventive measure being taken at seaports. While not new, police patrol at ports has increasingly involved partnerships among federal, state, and local law enforcement agencies, as well as private security firms and labor organizations. Seaport security varies considerably, depending upon the resources, statutory authority, and corporate policies of the individual seaport agencies.

We observed promising internal changes by the port police at the seaports we visited to prevent terrorism. These changes included the hiring of additional port police officers, improved training, additional surveillance responsibilities, intensified random patrol and check points, greater collaboration with private security, the building of new port police command centers at some ports, the creation of anti-terror and intelligence units, the switch to certified/sworn officers in some ports, the provision of new equipment to port police (e.g., portable radiation detectors to wear on a service belt), and the expansion of specialized units (e.g., K-9 units, explosive detection teams, and dive teams). We observed promising examples of collaboration among law enforcement agencies at the seaports we visited, including the Port of Boston's multi-jurisdictional effort to secure Liquefied Natural Gas tankers that enter the Port of Boston,

Galveston's multi-agency dive team, Jacksonville's MOU which provides operational control of both sheriff's deputies and private security guards to the port's Director of Security, the Port of Los Angeles Operation Archangel program to identify and protect critical assets, the Port of New Orleans multi-jurisdictional effort to secure cruise ships, the Port of San Diego Blue Force Tracking System to distinguish between law enforcement agency vessels and commercial and recreational vessels, and Savannah's multi-jurisdictional effort to secure ammonia ships in the Port of Savannah. We also observed several promising examples of interagency cooperation at the seaports we visited. In Long Beach, the police department has established a Harbor Unit that works closely with non-commissioned security personnel from the port. At the Port of Los Angeles, the Sea Marshals Unit (comprised of divers from the Coast Guard and the Los Angeles Port Police) conduct joint dive operations to protect ships and inspect critical infrastructure.

Fifth, interagency operational centers can greatly aid jurisdictions in preventing attacks against seaports. Various federal agencies have developed interagency operational centers at certain port locations. These are centers where multiple federal (and in some case, state and local) agencies are co-located in one facility and work together to monitor maritime security and plan related operations. The evaluation team visited four of these centers.

The Port of Charleston has the Charleston Harbor Operation Center (CHOC), commonly known as Project SeaHawk. SeaHawk is a multi-million–dollar, multi-agency, coordinated pilot effort, under the auspices of the U.S. Attorney. The purpose of SeaHawk is to create a unified law enforcement and intelligence operation to deter and prevent acts of terrorism. This includes managing a joint operations center to track maritime and other transportation operations in the Port of Charleston, establishing an interoperable system for data sharing and intelligence gathering, and providing a test bed for innovative concepts, initiatives, and equipment related to port security. All SeaHawk members meet daily to allocate resources to the most appropriate assignments. An intelligence unit combines intermodal transportation and harbor security data—including video camera feeds, radar, and thermal imaging—along with information about crews and cargo, to assess potential threats. A marine unit is involved with escorting vessels, providing security training, reaching out to community members, and boarding suspicious vessels.

The Port of Miami and Port of Everglades have been piloting Project Hawkeye. This project provides the Coast Guard with a system of cameras and sensors to identify and track vessels in harbor and coastal waters. Images from Hawkeye's radar sensors and long-range cameras are viewed on displays at the command center. This information is combined with data from an automatic identification system. This system can learn the normal port activities and identify deviations from normal, alerting the Coast Guard to anomalies. With this information, the Coast Guard can make better decisions about which vessels should be inspected.

San Diego has the San Diego Second Command Center-Joint (SCC-J). SCC-J co-locates representatives of local, state and federal agencies and arms them with smart technology to close port security gaps and increase port-level maritime domain awareness. The agencies share access to information provided by all participating agencies, allowing them to coordinate planning and response to critical incidents and complement each agency's capabilities.

In Virginia, the Joint Harbor Operations Center involves representatives of the Coast Guard and the Navy co-locating in one Coast Guard facility, sharing intelligence information and coordinating operations. The primary focus is on security information related to force protection for the Navy. Inside the center, homeland security personnel capture radar and sonar signals, track video and vehicle tracking data, take phone calls from the field, listen to radio traffic from patrols and commercial ships at sea, and break down classified intelligence information. About 50 Coast Guard and Navy personnel maintain a 24-hour watch on the waterways, bridges, tunnels and ports in Virginia.

(3) *Preparedness:* We identified a number of promising practices in the area of preparing for attacks against ports, including:

- Training
- Field exercises
- M*odels, Simulations, and Games (MS&G)*

One key element of preparing a port for an attack is to provide training. Providing awareness training to all port personnel on security issues helps to ensure that there will be more people who will notice something that is out of place. This is a fairly low-cost best practice. We observed a number of examples of promising practices in the area of local training in port security issues. Earlier we described the Port of Charleston's Project Seahawk. An added advantage of having Project Seahawk in Charleston is the availability of exceptional facilities for training. At the Port of Houston, training has been provided to all employees concerning requirements of the Maritime Transportation Security Act. In addition, training has been provided to private security guards and Terminal Security Officers. The Jacksonville Port Authority pays for members of the Jacksonville Sheriff's Office to attend seaport security training. Port Police in Los Angeles have established a security awareness training program, aimed at educating port employees and community members concerning the signs of potential terrorist threats and how to report them. Also, an important and sometimes less emphasized part of port policing is the need to practice and train at a firearms range.

Another key element of preparing a port for an attack is field exercises that simulate a potential threat, attack, or incident. These exercises play out scenarios such as the explosion of a "dirty bomb" that releases radioactive materials. Exercises can vary in size and scope and can test specific aspects of a terrorism response plan. Training and field exercises can involve dozens of federal, state, and local agencies including law enforcement, fire and emergency management, and other first responders. The exercise may also require close coordination across many jurisdictions, raising issues about how agency personnel can communicate effectively when they have different chains of command, communication systems, operating procedures, and equipment. Our team observed exemplary exercise programs at the Port of Savannah, which holds one-day multi-layered training exercises designed to refine, rehearse and validate homeland security plans.

While field exercises are very important for building preparedness, they can be very expensive and time-consuming. Another option to increase preparedness is the use of computer simulation exercises. The Port of Jacksonville has used computer simulations of a terrorist bombing of a major commercial bulk and container terminal to assess the seaport's emergency

response and evacuation plan. **A number of the sites we visited also are involved in the National Exercise Program** (NEP) and the associated Top Officials (TOPOFF) National Exercise Series to increase preparedness. The ports we visited have found the NEP useful in facilitating collaboration among port partners at all levels of government, and providing a means to conduct "full-scale, full-system tests" of collective preparedness, interoperability, and collaboration.

A third approach to increasing preparedness our team observed was the use of *Models, Simulations, and Games (MS&G)*. Ports are increasingly using MS&G to better prepare first responders to respond to an attack against seaports. MS&G can allow local officials to inexpensively plan for low-frequency, high-impact events. It fits their budgetary concerns, and ideally can disseminate information learned in large exercises to smaller entities. Some of the ports we visited have been working with games that simulate reactions to biological and radiological events, strategic incident commander games, the coordination problems associated with mass casualty medical triage, and even practice of medical treatment on simulated human bodies. MS&G can allow participants to respond as a team in real time to simulated emergency scenarios lasting two to eight hours. Models, simulations, and games also track participants' responses and provide real-time assessments of their expected actions, which permits each jurisdiction to determine strengths and areas of concern in advance of a real emergency. Most interestingly, MS&G can approximate real conditions and allow personnel to "experience" dangerous events without exposing them or their environment to actual hazards, without consuming actual resources (e.g., personal protective equipment kits), and with little or no possibility of accidental injury to participants.

(4) *Response After an Attack:* Responding after an attack is the next key element for increasing seaport security. We identified a number of promising practices, including:

- An Incident/Unified Command approach
- Exercise and training
- Team responses

First**,** many of the ports we visited used the Incident Command System to deal with the uncertainty and fast collaborative/multi-agency action associated with responding to an attack against a port. Under this system, the agency chosen to oversee emergency operations depends on the nature and location of the event. A "Unified Command" could be established, in which agency managers share decision-making responsibility within a group, with individual agencies maintaining operational control over their own assets and personnel. This system allows agencies to adapt to changing situations by avoiding a rigid organizational structure, but it hinges on informal trust, cooperation, and institutional knowledge about which agency leads under what circumstances.

Second, exercises and training programs are among the key activities that a seaport can undertake to prepare to respond to a terrorist attack. Under this heading, we identified a number of promising practices, including Seattle's Marine Terrorism Response (MTR) Project, the Maritime Incident Resources Training Partnership (MIRT) in Boston, and local participation in the Department of Homeland Security-developed Port Security Exercise Training Program (PortSTEP).

With DHS funding, the Port of Seattle developed the extensive exercise and training program called the MTR Project. The MTR Project includes a preparedness plan, a response plan, and a field operations guide for emergency responders. The MTR plan includes web-based training, classroom/vessel training, and field exercises. The MIRT at the Port of Boston is an initiative started by local fire departments. The main goal of MIRT is to provide training to local fire departments and support agencies that are called upon to respond to shipboard fires as well as other maritime emergencies that could occur in Massachusetts waters. Another goal of MIRT members is to expand current response capabilities and enhance maritime safety through regular training and field exercises using a unified command system.

Another promising practice in the area of exercise and training we reviewed is local implementation of PortSTEP. The Transportation Security Administration and the Coast Guard developed PortSTEP to help ports meet the mandates of the Maritime Transportation Security Act. PortSTEP brings together government and private-sector officials responsible for maritime transportation and commerce, emergency response, and land transit. Officials participate in scenarios intended to reflect the types of incidents most likely to occur in the current terrorist threat environment. A number of our research sites have been involved in PortSTEP and consider it a promising practice.

Third, the experts we talked with on our site visits pointed to the need for team response—strong partnerships and the formation of teams that would respond to a terrorism incident at a seaport. First, the LA CERT (Community Emergency Response Team) Model stood out as a promising practice in the area of team responses. Rather than using traditional emergency response models, Los Angeles port officials have been working with the Los Angeles Fire Department (LAFD) to train civilians to be first responders in vulnerable target areas. Making use of the natural inclinations of citizens to help, the LAFD train populations in vulnerable port areas on how to help themselves and others until professional emergency response personnel can arrive at the port. The Federal Emergency Management Agency (FEMA) adopted the LA CERT model and since the September 11 attacks has been directing grants to fund civilian CERT programs in all 50 states. The CERT Program educates people about preparedness for disasters that may impact their area and trains them in basic disaster response skills.

Another important team response is the Maritime Safety and Security Teams (MSSTs). MSSTs are a Coast Guard rapid response force assigned to vital ports and capable of nationwide deployment via air, ground or sea transportation to meet emerging threats. MSSTs have unique capabilities, including explosive-detection dogs, personnel trained to conduct fast-roping deployments from a helicopter to a hostile vessel, and anti-terrorism/force protection. The Port of Seattle was the first port in the nation to get an MSST stationed at its port.

Other promising team responses to responding to an attack were found in Boston, Charleston, Houston, and Virginia. In Virginia they have developed the Maritime Incident Resources Training (MIRT) partnership, a team of fire fighters who have experience in fighting shipboard fires and have purchased equipment that can be used in extinguishing such fires. MIRT has also developed a training curriculum used by hundreds of firefighters and other

professionals from the Norfolk area as well as from all over the United States. As discussed earlier, the Port of Boston has also adopted MIRT.

The Port of Charleston has developed its Port Emergency Information Center for collecting and distributing information to port stakeholders concerning status of emergencies and what is required to reopen the shipping channel. The Port of Charleston has a Port Operations Emergency Center for working with affected agencies to coordinate responses to emergencies. The Port has also developed a Marine Fire Fighting Protocol to train local fire fighters on how to fight fires on the waterfront.

The Port of Houston has a Channel Industries Mutual Aid (CIMA) group. CIMA is a nonprofit organization combining the firefighting, rescue, hazardous material handling, and emergency medical capabilities of the refining and petrochemical industry in the Houston Ship channel area. CIMA provides cooperative assistance and expertise for all kinds of emergencies. CIMA maintains groups of highly trained emergency personnel and a well-maintained collection of equipment. The Port of Houston has also developed a system to divide the ship channel into nine areas, so that damage can be assessed separately and recovery plans can be coordinated.

(5) Recovery after an attack: Recovery, the final key element of seaport security, includes the need to **a**ssure continuity of port operations to maintain vital commerce**,** with a focus on expediting the recovery of maritime infrastructure, transportation systems, and affected maritime communities. Compared to the other four areas already discussed, we did not learn about very many promising practices in the area of recovery on our site visits. Nevertheless, we did learn about promising practices in establishing recovery implementation plans in:

- Galveston/Houston
- Los Angeles and Seattle
- Using a consequence management approach to recovery in ports in Houston and Los Angeles

In the Houston/Galveston area, officials have established Port Coordination Centers (PCCs) to inform and advise on port operational and infrastructure needs, including security concerns that arise in the case of an emergency. The Centers can convene functionally in the case of a natural disaster, or geographically in the case of a security incident. Each PCC designates a liaison officer to the regional Port Coordination Team (PCT) in order to establish shipping priorities, manage the flow of vessel movements, preserve safety and security, and implement established emergency protocols. The PCT's role is to disseminate information concerning the nature of the threat, implement protective strategies, continue communication to update the strategies, and reopen the port in an orderly manner.

In Seattle the port authority has developed a business continuity plan that spells out how to decide which operations go back in business in which order. Also, at the Port of Los Angeles, the port authority has produced a business resumption plan to direct reopening of port after it has been closed due to a terrorist attack.

Consequence management involves a formal process for the restoration function after a catastrophe and addresses the ways and means to alleviate the effects of a catastrophe. In Chris

Seiple's (1997) article on consequence management,[3] a number of his recommendations are relevant for seaports to consider in adopting a consequence management model, including: Establishing coordination mechanisms to oversee the entire immediate response before federal assets arrive, planning for the use of federal assets to augment the existing response, examining the role of the military's reserves in a tiered response between the first responders and the arrival of federal help, planning for surge capacities that will be needed for different types of response, developing plans for tactical coordination at the incident, developing evacuation plans, deciding who will handle the information campaign, planning for the role of medical facilities, and ensuring that fire and police departments are prepared to work together.

Based on our discussion with various ports officials, a number of recommendations emerged in the area of consequence management. First, ports should consider adopting a consequence management awareness/training program and a certification process for all levels of response to avoid disparate approaches which could inhibit communication and coordination. Second, it is important to identify, train, and mentor individuals within organizations on consequence management. Third, ports should develop a tiered continuum of response. All national assets, unless already deployed to potential terrorist targets, are generally not going to be able to respond to an incident within 6 to 12 hours. Local responders will have to carry the burden of the immediate response. Seaports need to consider completing exercises geared towards consequence management and business resumption. For example, the Port Authority of New York and New Jersey has done consequence management training for its seaport personnel and stakeholders through a DHS-sponsored "war game." Also, ports in Houston and Los Angeles are working towards a consequence management approach.

IV. Conclusion

Our research provides seaport officials with ideas and data to help adopt, modify or replace their security protocols, programs and other aspects of their security operations. As in many operational areas, key ingredients for successful security operations relate to port leadership, funding/resources, organizational structures that integrate security into key operational aspects of the port, communication systems and information sharing, qualified professional staff, training, team work, and clarity of mission. Other important features of port security operations include the use of incident management systems, attention to communications interoperability, public/media relations, written policies, plans and procedures, and mutual aid agreements. More specifically, the better seaport security operations often had elements of all five our general study areas of:

- Improving *awareness* of threats to a port
- *Prevention* against an attack on a port
- Enhancing *preparedness* for an attack against a port
- *Response* after an attack
- *Recovery* after an attack.

<u>Awareness of threats to seaports</u>

[3] Seiple, C (1997). Domestic Response to Weapons of Mass Destruction. *Parameters*, Autumn 1997: 119-34.

In raising maritime awareness of terrorism, seaport officials should consider active involvement in an Area Maritime Security Committee (AMSC) or other similar committee/council to help raise maritime awareness of terrorism; developing a port intelligence team or special port security unit within an existing homeland security center, managing or structuring port data to integrate security into port operations to assure that security personnel have the necessary information they need, and working with the closest state fusion center and/or terrorism task force/council to raise the profile of port security.

Prevention against an attack on a port

In preventing attacks against ports, seaport officials should consider improving a range of physical security/infrastructure improvements, tightening protocols and processes limiting entry to seaports, adopting new technology detection/inspection systems, enhancing law enforcement-related activities, and fostering the advancement of interagency operational centers. While the interagency operational centers at the Ports of Charleston, Miami/Everglades, San Diego and Virginia are impressive, they are expensive and take years to become fully operational. Nevertheless, this report documents important features at each of these centers that could be adopted individually without the development on an entire center.

Enhancing preparedness for an attack against a port

In preparing for an attack against a port, we identified a number of promising practices that ports should consider adopting such as port security specific training; field exercises; and Models, Simulations, and Games (MS&G). While some of these are very extensive, at least some elements of the promising practices in this area can be implemented in almost all ports. For example, awareness training to all port personnel on security issues is a low cost approach that allows for more people to notice something that is out of place. Field exercises are excellent preparatory efforts that simulate a potential attack and test aspects of the port's terrorism response plan. Similarly, MS&G can provide real-time assessments of port personnel during a simulated emergency without exposing port personnel or their environment to actual hazards, without consuming actual expensive protective equipment kits and with little possibility of accidental injury to participants.

Response after an attack

In responding to an attack, seaport officials should consider the use an Incident/Unified Command approach to allow agencies to adapt to changing situations by avoiding a rigid organizational structure. Once again, exercises and training programs are important and among the key activities that a seaport can do to prepare to respond to a terrorist attack. Good examples of this area can be found in this report, including: Seattle's Marine Terrorism Response (MTR) Project, the Maritime Incident Resources Training Partnership (MIRT) in Boston, and local participation in the DHS developed Port Security Exercise Training Program (PortSTEP). Team responses are another critical element of an effective response to an attack against a seaport. The LA CERT (Community Emergency Response Team) Model stood out as a promising practice in the area of team responses. Other promising responses for ports to look at include team responses in the ports of Boston, Charleston, Houston, and Virginia. These promising team responses are being used help coordinate teams of fire fighters to combat shipboard fires, emergency information centers for collating and distributing emergency information to port

stakeholders, and public-private partnerships to provide specialized equipment to handle certain emergencies.

Recovery after an attack

In the final stage of recovery after an attack, seaport officials should consider establishing recovery implementation plans and using a consequence management approach to recovery. Compared to the other four areas already discussed, on our site visits we did not observe or learn about very many promising practices in the area of recovery. This is unfortunate, for actions such as these steps could go a long way in preserving life, property, the environment, and social, economic, and political structures, as well as in restoring order and essential services for those who live and work within the maritime domain. From our site visits our team learned about some general guidelines in coordinating recovery after an attack on a port, including: Seaport officials need to consider establishing a coordination mechanisms to oversee the entire immediate response before federal assets arrive, planning for the use of federal assets to augment the existing response, examining the role of the military's reserves in a tiered response between the first responders and the arrival of federal help, planning for surge capacities that will be needed for different types of responses, developing plans for tactical coordination at the incident, developing evacuation plans, planning for who will handle the information campaign, planning for the role of medical facilities, and ensuring that fire and police departments are prepared to work together. These are some basic steps that many ports can adopt. Recovery efforts could also be potentially advanced through the adoption of a consequence management approach.

It is our hope that this project will provide port officials with valuable information for improving their ability to provide security in and around ports, prepare for and respond to terrorism incidents, and develop partnerships that leverage the various public and private resources that may be at their disposal.

In the end there are no magic bullets to assist the port community with the monumental assignment of protecting the Nation's port against a terrorist attack. The complex task of coordinating and working with the many involved agencies to provide the required security to our nation's seaports will not easily be accomplished. This report provided a review of innovative practices occurring at local seaports so at a minimum ports can at least start learning from each other to take on this colossal task, rather than developing new strategies from "first principles." This report shows that security improvements are being made in some seaports but that gaps in program design and implementation still remain. While much work still needs to be done, seaports have at least made some strong in-roads into improving security. As outlined in a recent NIJ study (Davis, Ortiz, Rowe, Broz, Rigakos, and Collins, 2006 at http://www.asisonline.org/foundation/noframe/mall.pdf), it appears if the mall security community has made much less progress. Ports can learn how to fill some of these gaps by learning from the experience of the ports discussed in this report. Learning from other ports in the areas of awareness building, prevention, preparedness, response and recovery after an attack is a step in the right direction of making all of the seaports in the US safer.

MAIN REPORT

Protecting America's Ports: Promising Practices

I. Introduction

The terrorist attacks on the World Trade Center and the Pentagon on September 11, 2001 brought America to attention regarding the vulnerability of its infrastructure in general and its transportation system in particular. It is widely known that, immediately following those attacks, the United States shut down its entire air traffic system for several days. It is less widely known, however, that the government also temporarily halted the maritime transportation system, preventing ships approaching U.S. shores from reaching their destinations. This closure was in recognition of the fact that, just as airplanes could serve as weapons, so could ships and their cargo.[4]

Attention has been paid. Soon after 9/11, a Council on Foreign Relations report by former U.S. Senators Gary Hart and Warren B. Rudman, recognizing the serious threats posed to national security by the vulnerability of our ports, recommended that the United States "recalibrate the agenda for transportation security [because] the vulnerabilities are greater and the stakes are higher in the sea and land modes than in commercial aviation." Similarly, the 9/11 Commission (National Commission on Terrorist Attacks Upon the United States, 2004, p. 391) reported that, "While commercial aviation remains a possible target, terrorists may turn their attention to other modes. Opportunities to do harm are as great, or greater, in maritime and surface transportation."

Responding to these alarms, government officials and security experts have increasingly attended to the potential threats against the maritime transportation system. The concerns are of two basic types. First, transporting something from one place to another—the very activity that ports facilitate—would be attractive to terrorists, since they could use a port as a conduit through which to build an arsenal within the nation's borders. Second, ports themselves present attractive targets for terrorists. Aggregating the scenarios hypothesized by various researchers (Fritelli, 2005, 5-6; Greenberg, et al. A, 2006: 27; Campbell and Gunararna, 2003: 70-89; Herbert-Burns, 2005: 163-169; Sinai, 2004: 63-64; Percival, 2005: 10-13; and Clarke, 2005) provides a terrifying list of maritime terrorist threats.[5] Among other things, terrorists could:

---

[4] We had been warned. As early as 1999, a special commission comprised of representatives of 15 federal agencies evaluated the state of security at U.S. seaports. The result of that body, the *Report of the Interagency Commission on Crime and Security in U.S. Seaports* (2000), concluded, after examining a limited number of ports, that security was generally inadequate and that the vulnerability of seaports to a terrorist attack was high.

[5] For simplicity, we omit elaborating on the specific tactics that could be used in each scenario, including improvised explosive devices (IEDs); boat-borne or water-borne devices; standoff

- Use commercial cargo containers to smuggle terrorists, nuclear, chemical, or biological weapons, components thereof, or other dangerous materials into the United States;
- Use a "Trojan horse," such as a fishing trawler, resupply ship, tug, or similar innocuous-looking vessel, to transport weapons and other battle-related materiel;
- Seize control of a large commercial cargo ship and use it as a collision weapon for destroying a bridge or refinery located on the waterfront;
- Hijack a vessel and hold it for ransom to support a campaign of political violence directed toward ethnic, ideological, religious, or separatist designs;
- Sink a large commercial cargo ship in a major shipping channel, thereby blocking traffic to and from the port;
- Attack or hijack a large ship containing a volatile fuel (such as liquefied natural gas (LNG) or liquefied petroleum gas (LPG) and detonate the fuel to cause a massive in-port explosion;
- An attack designed to disrupt the world oil trade and cause large-scale environmental damage;
- Seize control of a ferry (which can carry hundreds of passengers) or a cruise ship (which can carry more than 3,000 passengers many of whom are likely to be U.S. citizens) and threaten the deaths of the passengers if a demand is not met;
- Attack U.S. Navy ships in an attempt to kill U.S. military personnel, damage or destroy a valuable U.S. military asset, and (in the case of nuclear-powered ships) cause a radiological release;
- Attack vessels or ports used to supply military operations overseas, interfering with those operations;
- Directly target a cruise liner or passenger ferry to cause mass casualties by contaminating the ship's food supply, detonating an improved explosive device (IED), or ramming the vessel with a fast-approach, small attack craft; and/or
- Use land around a port to stage attacks on bridges, refineries located on the waterfront, or other port facilities.

As described at greater length below, several government programs have been implemented since the attacks of 9/11 to improve the ability to prevent terrorist attacks on the nation's ports. Arguably the most important development was the passage of the Maritime Transportation Security Act (MTSA), signed into law by President Bush on November 25, 2002 and implemented on July 1, 2004. In addition, the U.S. Coast Guard and the U.S Customs Bureau, now called Customs and Border Protection (CBP), have instituted several maritime security measures.

Nevertheless, even these intensified federal efforts are not, in and of themselves, sufficient to provide sufficient security in and around our ports. Unlike many countries, the United States has no national port authority. Thus, as described below, because of the size and structure of the maritime system, the involvement of local law enforcement and private security

---

weapon attacks (e.g., mortar, grenade launcher, heavy rifle, shaped charge, etc.); suicide bombings on board a ship; and use of submersible parasitic devices.

will be required if our defenses are to be successful. Unfortunately, little is known about the nature of anti-terrorist activities in the nation's ports or what "promising practices" might deserve further scrutiny and testing. Such information, if shared, could provide assistance to local agencies, both public and private, in improving the security of America's ports.

To help fill this gap in our knowledge, and to make such useful information available to those concerned with protecting our ports, the Police Executive Research Forum sought and received funding from the National Institute of Justice to conduct a study designed to identify "promising practices" used by local law enforcement and private security agencies to prevent America's deep-draft ports from terrorist attacks. This report provides a summary of that study.

The following section of the report provides an overview of the maritime environment in the United States, the structure of responsibilities of protecting the nation's ports, and the nature of the terrorist risks in those ports. The third section summarizes the methodology used in the project, including discussion of the ports visited and data collection procedures. The fourth section presents the essential findings of the study—the "promising practices" being implemented in the ports visited. Finally, the fifth section provides a summary of the report and its major conclusions.

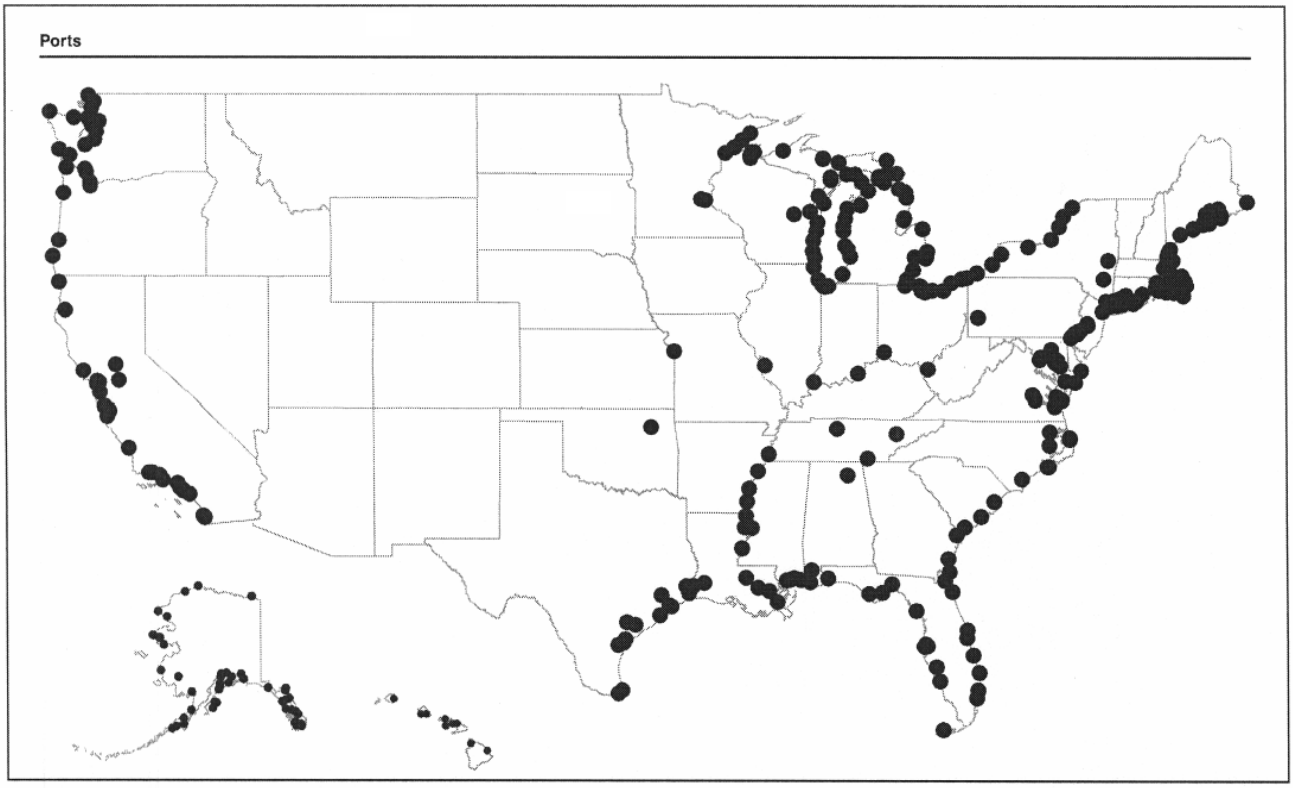
II. Literature Review

Background on the Maritime Environment

America is, essentially, an island nation. As such, it is largely dependent on its 361 ports: 185 "deep water" and 176 "inland." (A map of the 361 American ports is provided in Figure 1 on the following page.) Located on these ports are approximately 3,700 terminals and facilities. According to the Council on Foreign Relations (2002), fully 95 percent of overseas commerce (and 100 percent of certain commodities, such as foreign oil) comes by ship through our ports. Approximately 8,000 ships with foreign flags make 51,000 calls on U.S. ports each year, carrying approximately 1.1 billion tons of goods in 11.5 million containers, 156 million tons of hazardous materials, and 175 billion gallons of oil and other fuels. Every year approximately 9 million cargo containers arrive at America's seaports—about 26,000 a day (Ervin, 2006: 118) Further, there are over 6.5 million cruise ship passengers passing through U.S. ports each year, over 80 percent of whom are American citizens. Ferry services operate in approximately 30 urban areas, serving more than 66 million passengers every year (American Public Transportation Association, 2006: 61.) Thirteen commercial ports have been designated by the Departments of Defense and Transportation as "strategic," because in the event of a large-scale military deployment, DOD would transport more than 95 percent of all equipment and supplies needed for military operations by sea.

In addition to keeping America's goods on the move, our ports also help stimulate America's economy. Almost 16 million Americans work in port-related jobs—jobs that provide $515 billion in annual income and $210 billion in federal, state, and local taxes. Port activity also contributes more than $780 billion to the Gross Domestic Product.

Figure 1. Ports of the United States



Source: GAO presentation of Bureau of Transportation statistics, TSA, and FTA data.

Harrald, et al. (2004) describe America's ports as a "system of systems":

> The maritime trade has evolved into a segregated set of very highly specialized systems. Port facilities have adapted to these disparate systems and a major port may be viewed as a collection of loosely coupled subsystems. High-value cargo is shipped in containers, carried by container ships that must be loaded and unloaded by multi-million-dollar high-speed cranes at container facilities specifically designed to efficiently transfer these containers to other transportation modes…. Automobiles are shipped on specially designed car carriers to specific automobile handling facilities. Cruise ships operate out of cruise ship facilities designed to efficiently embark and disembark thousands of passengers. In several major ports commuters and tourists travel between ferry terminals on high-speed, high-capacity ferries. Petroleum cargo is transported between refineries and petroleum facilities, and 100 percent of imported foreign crude oil and Alaskan crude oil is transported by ship. Bulk cargo (grains, ores, etc.) is served by bulk facilities which handle the imports of critical commodities and transship all U.S. agricultural exports. Internationally, these cargoes are carried on deep draft vessels, foreign flag vessels typically operating in extremely competitive spot markets. Domestically, the U.S. towboat industry transports bulk cargoes on board thousand of barges.

Harrald and colleagues further point out that:

> America's ports are critical nodes in the specialized, complex economic inter-modal subsystems that move goods and cargo around the world. In port, they point out, cargo and passengers are transferred to and from the maritime mode from/to other transportation modes (e.g., rail, road, or pipeline).

The complex nature of ports and the port authorities that govern them, including the variation in public and private ownership, the involvement of multiple governmental and private agencies, and the variation in levels and scopes of authority, makes the provision of security in our ports a tremendously difficult task, mandating the need for partnerships among federal, state, and local law enforcement agencies, as well as private security firms and labor organizations. Most of the responsibility falls to public seaport agencies. Such agencies vary significantly in structure, operation, and governance, not only *between* but also not infrequently *within* individual states. Some are, in fact, "port authorities," in the sense of being autonomous or quasi-autonomous, self-sustaining public corporations. Others, however, are integral administrative divisions of state, county, or municipal government. Independent port or navigation districts constituted as "special purpose" political subdivisions of state government exist in California, Florida, Ohio, Washington, Oregon, Louisiana, and Texas. Bi-state agencies created as a result of Congressionally-sanctioned compacts between state governments include the Delaware River Port Authority and the Port Authority of New York and New Jersey (Nagle, 2002).

The jurisdiction of most seaport agencies is limited to a single port, but in a few cases, such as the North Carolina and South Carolina State Ports Authorities and the Harbors Division of the Hawaii Department of Transportation, they may have jurisdiction over two or more ports. The range of permitted authority of these agencies also varies; this authority may extend to airports, bridges, tunnels, commuter rail systems, inland river or shallow draft terminals, industrial parks, foreign-trade zones, world trade centers, terminal or short-line railroads, marinas, and public recreational facilities. Many are given police powers, at least to the extent of maintaining security and enforcing board-approved ordinances on properties owned by seaport agencies (Nagle, 2002).

In terms of port operation and administration, there are two broad classifications of maritime ports—"operating ports" and "landlord ports."[6] The distinction between these two types of ports lies in their degree of operational responsibility. "Operating ports" manage and execute the daily operations typically associated with a maritime port. In a "landlord port," operational activities are performed by terminal operators, who lease quayside property from the port.

The operational functions performed by "operating ports" and terminal operators typically include the servicing of cargo vessels, the lading and unlading of cargo, the storage of cargo, the inspection of suspicious cargo, and the pick-up and drop-off of cargo from/to inland origin and destination points. Operating ports and terminal operators sell their services to carriers, who are the owners/operators of the cargo vessels (ships), trucks, and rail lines that

[6] These classifications are "ideal types," exemplifying the distinguishing features of the two basic types of ports. In reality, the world is much more complicated. There are many hybrid ports, also known as "limited operating ports," in which the port manages and operates certain terminal facilities (or functions) but leases other facilities (or functions) to terminal operators.

carry goods to and from the port. According to the U.S. Maritime Administration (2005: 1), public port authorities only own approximately one-third of the deep-draft marine terminal facilities in the United States.[7] Further, according to the Congressional Research Service, at the seventeen largest U.S. container ports, 45 terminals (66 percent) were operated by a foreign-based company, five terminals (7 percent) were operated by a joint venture between a domestic and foreign-based company, and 18 terminals (26 percent) were operated by a purely domestic terminal operating company (Fritelli and Lake, 2006 3). Several of those ports have no U.S.-based container operators.[8]

Ports also vary according to their structure of governance. Some ports are operated under the auspices of a port authority that is a public entity of the state or local government, which owns the property. Other port authorities are autonomous or semi-autonomous, self-sustaining public corporations. Others are divisions of state, county, or municipal government. Finally, there are a small number of ports that are privately owned, independent of any agency of government.

Finally, ports can be categorized according to how they arrange for law enforcement coverage (this is regardless of whether private security is utilized in certain circumstances):

- Some ports (such as San Diego, Los Angeles, Virginia, New York/New Jersey, Charleston, New Orleans, Boston, and others) have their own police department.
- Other ports (such as Jacksonville, Tampa, and Fort Lauderdale) contract with local sheriff's agencies for law enforcement while relying on private security for order maintenance.
- Some ports (such as Miami) have local law enforcement agencies situated on their premises.
- Some ports (such as Baltimore) depend upon a state law enforcement agency for law enforcement coverage.
- Other ports (such as Long Beach) rely on the local municipal police department for law enforcement but have their own quasi-law enforcement unit as well.
- Finally, some ports (such as Texas City) depend upon their own private guards and security agencies provided by local tenants for primary security, but call upon local law enforcement in emergencies.

There are several ways that activity in ports can be measured, including value of trade, tonnage, vessel calls, container traffic, passengers, and passenger ships visiting. For the purposes of this study, the number of containers and passengers best serve as indicators of

[7] Many of the privately-owned marine terminals are associated with the oil, gas, and chemical industries. In these cases, the waterside terminal may be a component of a larger industrial complex on land (GAO, 2006, p.2)

[8] "Most U.S. container terminals are managed by foreign companies because almost all of the container shipping lines are owned by foreign companies. Typically, a foreign container shipping line creates a U.S. subsidiary or a U.S. affiliate to operate the terminals at its busiest U.S. ports to better ensure service quality and control costs" (Fritelli and Lake, 2006: 4).

terrorist target potential. Table 1 provides information concerning the number of Ton Equivalent Units (TEUs)[9] handled by each port during calendar year 2004.[10]

Table 1. *Seaports, by 2004 Containers, Management Structure, and Policing Type*

Port	Rank	TEUs	Type of Port Governance
Los Angeles	1	7,321,440	**Landlord**
Long Beach	2	5,779,852	Landlord
New York/New Jersey	3	4,788,480	**Landlord**
Oakland	4	2,043,122	Landlord
Charleston	5	1,863,917	**Operating**
Port of Virginia	6	1,808,933	**Operating**
Tacoma	7	1,797,560	**Limited Operating**
Seattle	8	1,775,858	**Limited Operating**
Savannah	9	1,662,021	**Operating**
Houston	10	1,437,585	**Limited Operating**
Honolulu	11	1,041,455	Operating
Miami	12	1,009,500	Landlord
Jacksonville	13	727,660	Landlord
Port Everglades	14	653,628	Limited Operating
Baltimore	15	557,858	**Limited Operating**
Portland, OR	16	274,609	Limited Operating
New Orleans	17	258,468	**Landlord**
Palm Beach	18	226,002	Landlord
Gulfport	19	213,108	Landlord
Philadelphia	20	178,046	Landlord
Boston	21	175,679	**Operating**
Wilmington, DE	22	160,914	Operating
Wilmington, NC	23	104,122	**Operating**
San Diego	24	92,834	**Operating**
Freeport, TX	25	68,568	Operating
San Francisco	26	32,045	Operating
Galveston	27	10,291	**Landlord**
Port Canaveral	28	1,252	Landlord
Source: American Association of Port Authorities			
Boldface/highlighting indicates a port authority that has its own police department.			

As the table indicates, there are certain container "mega-ports," namely Los Angeles, Long Beach, New York/New Jersey, and Oakland, that handled more than two million TEUs in 2004. It is noteworthy that all of those are "landlord" ports, delegating responsibility for handling cargo to private tenants. Eight other ports, Charleston, Virginia, Tacoma, Seattle,

[9] A TEU is a standard linear measurement used in quantifying container traffic flows. As examples, one twenty-foot long container equals one TEU while one forty-foot container equals two TEUs.

[10] Data for 2005, although available, are distorted because the Port of New Orleans was closed for much of that year.

Savannah, Houston, Honolulu, and Miami, handled over one million TEUs, but less than two million. Sixteen other ports handled a significant number, but fewer than one million TEUs, of containers.

Table 2 provides a similar breakdown of the number of cruise passengers handled by each of the nation's major ports.

Table 2. *Seaports, by Passengers, Management Structure, and Policing Type*

		Passengers	**Type of Port Governance**
	Rank	**(1000s)**	
Miami	1	1,683	Landlord
Port Everglades	2	1,237	Limited Operating
Port Canaveral	3	1,230	Landlord
New York/New Jersey	4	548	**Landlord**
Los Angeles	5	435	**Landlord**
Galveston	6	433	**Landlord**
Long Beach	7	401	Landlord
Tampa	8	399	Landlord
New Orleans	9	396	**Landlord**
Seattle	10	291	**Limited Operating**
San Diego	11	172	**Operating**
Honolulu	12	170	
Jacksonville	13	113	Landlord
Baltimore	14	104	**Limited Operating**
Houston	15	91	**Limited Operating**
Whittier	16	88	Operating
San Francisco	17	85	Operating
Boston	18	73	**Operating**
Charleston	19	39	**Operating**
Philadelphia	20	30	Landlord
Mobile	21	29	Operating
Gulfport	22	3	Landlord
Source: United States Maritime Administration			
Boldface/highlighting indicates a port authority that has its own police department.			

Table 2 indicates that three ports, Miami, Port Everglades, and Port Canaveral, handled over one million passengers in 2004. Not surprisingly, all of these ports are in Florida. None of these ports has its own police department. Only the Port of Miami also handled more than 1 million TEUs of containers. Six ports, Los Angeles, Galveston, Long Beach, Tampa New Orleans, and Seattle, accommodated between approximately 300,000 to 600,000 passengers in 2004: All of these ports but Galveston handled at least a moderate number of containers as well.

Responsibilities for Port Security

Responsibility for security is spread widely among federal, state, and local law enforcement agencies, port authorities, and private security. In summary:

- The U.S. Coast Guard (USCG) has legal authority for enforcing security requirements at all U.S. seaports and waterways, as well as authority for several other areas, including maritime law enforcement and national security. The 45 Captains of the Port are responsible for enforcing this authority.
- U.S. Customs and Border Protection (CBP) is responsible for ensuring that all goods and persons entering and exiting the United States do so in accordance with all U.S. laws and regulations.
- The U.S. Immigration and Customs Enforcement (ICE) agency is responsible for the examination and inspection of all crews and passengers arriving on ships from ports outside the United States to ascertain their admissibility to the country.
- The Maritime Security Division of the Transportation Security Administration (TSA) is responsible for the development and implementation of the Transportation Worker Identification Credential (TWIC), which will be required as a common credential for all personnel requiring unescorted access to secure areas of facilities and vessels regulated by the Maritime Transportation and Security Act of 2002. In addition, in collaboration with the USCG, the TSA is responsible for developing and implementing the Port Security Exercise Training Program (known by the acronym PortSTEP), which is providing a series of port security training exercises and evaluation services for maritime and surface industry partners.
- Port authorities have general responsibility for maintaining security in their ports.
- The U.S. Department of Agriculture oversees the import and export of agricultural products.
- The U. S. Food and Drug Administration (FDA) inspects a wide range of products, from pharmaceuticals to television screens and dinner plates with lead glaze.
- The U.S. Department of Commerce (DOC) collects the Shipper's Export Declaration (SED) and issues licenses for items on the Commerce Control List.
- The U.S. Maritime Administration (MARAD) operates the Port and Cargo Security Program.
- The U. S. Department of Defense (DOD) becomes involved in the Strategic Ports in case of a military mobilization.
- The Federal Maritime Commission regulates rates and licenses.
- The FBI, DEA, and ATF also become involved in cases under their jurisdiction.
- State law enforcement agencies, in some ports, have varying degrees of responsibility for security in port facilities.
- Municipal/county law enforcement agencies have responsibility for port security on those ports that are part of local government, or that contract for their assistance. In other cases, such agencies may serve as backup support in case of emergencies.
- Port authority police, hired by a Port Authority, have responsibility for enforcing laws and crime prevention on port property.
- Port authority security guards, hired by a Port authority, have responsibility for maintaining security on port property.

- Port security employees, also hired by Port Authorities, have responsibility for funding and coordinating port security efforts on port property.
- Private security guards, hired by terminal operators/tenants, have responsibility within the confines of the leased areas.
- Terminal operators, whether by hiring private security guards or by other means, are responsible for security in the facilities they lease or own.

Ports at Risk

It is impossible to allocate sufficient resources to protect all possible targets of terrorist attacks with equal vigor. It is standard policy, therefore, to prioritize potential targets according to a "risk assessment." Such assessments[11] customarily calculate "risk" ("the potential for some unwanted event to occur") as a function of three factors:

- "Threat," defined as the "capability and intention of an adversary or competitor to undertake actions that have consequences detrimental to an organization or enterprise";
- "Vulnerability," defined as "weakness that can be exploited by an adversary"; and
- "Consequences," defined as "adverse effects from the loss of an asset."

In order to understand the risk of terrorist attacks on our nation's ports, it is worthwhile to assess our ports with regard to the three aspects of risk.

Threat. Al Qaeda leader Osama bin Laden has made no secret that he sees the destruction of the U.S. economy as one of his goals: "If their economy is finished, they will become too busy to enslave oppressed people. It is very important to concentrate on hitting the U.S. economy with every available means" (Agence France-Presse, 2001). History provides the clearest evidence of the threat of terrorism against the maritime transportation system. A few examples:

- On October 12, 2000, almost a year before 9/11, the guided missile destroyer USS *Cole* was attacked by al Qaeda terrorists while refueling in the Yemeni port of Aden, killing 17 sailors and injuring 39 others.
- About one year after 9/11, on October 6, 2002, the French oil tanker *Limburg* was rammed by a small boat filled with explosives as it was headed into the same port. The vessel caught on fire and approximately 90,000 barrels of crude oil were spilled into the Gulf of Aden. Again, al Qaeda claimed responsibility for the attack.
- On March 14, 2004 there were two suicide bomb explosions in the Israeli port of Ashdod. The bombers had hidden inside an empty container, which had entered the port from Gaza. Ten people were killed, including the bombers.

Scholars have generally agreed that the maritime system faces serious threats from terrorism. Stephen Flynn, a former Coast Guard Commander, now at the Council on Foreign Relations, says in America the Vulnerable (2004:83-84):

[11] See, for example, Parnell, Dillon-Merrill, and Bresnick (2006); President's Commission on Crucial Infrastructure Protection (1997); and U.S. Government Accountability Office (2005).

> …containers are going to be exploited as a poor man's missile. The question is when, not if.

Graham Allison, founding dean of the John F. Kennedy School of Government, says in Nuclear Terrorism (2004: 106-107):

> The nuclear weapon that terrorists would use in the first attack on the United States is far more likely to arrive in a cargo container than on the tip of a missile.

The U.S. Government Accountability Office (2004) stated:

> Since the terrorist attacks of September 11, 2001, the nation's 361 ports have increasingly been viewed as potential targets for future attacks for many reasons. For example, security experts remain concerned about the potential for using the maritime transportation system as a conduit for smuggling weapons of mass destruction or other dangerous materials into the country.

Vulnerability. Jay Etta Hecker, Director of Physical Infrastructure Issues at the U.S. Government Accounting Office, testified before a Congressional committee (United States Government Accounting Office, 2002):

> 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.

Echoing the same theme, Robert Bonner, Commissioner of the U.S. Customs Service, said on August 26, 2002:

> There is virtually no security for what is the primary system to transport global trade.

Former U.S. Coast Guard Commandant Admiral James Loy (Loy and Ross, 2002) stated that of all transportation modes, the maritime industry is the most valuable and the most vulnerable, and that "terrorist threats have a natural gateway into America via the marine transportation system."

Allison (2004: 107) supported this argument:

> Every day, 30,000 trucks, 6,500 rail cars, and 140 ships deliver more than 50,000 cargo containers with more than 500,000 items from around the globe….Fewer than one in 20 of these containers is inspected upon arrival.

Flynn (2004: 89) concurs:

On average, overseas containers will pass through 17 intermediate points before they arrive at their final U.S. destination, and often their contents come from several locations before they are even loaded into the box. Nearly 40 percent of all containers shipped to the United States have such an assortment of contents that they are the maritime transportation equivalent of the back of a UPS van.

Recent events bear out these concerns. To name a few:

- ABC News managed to smuggle 15 pounds of depleted uranium from Istanbul, Turkey to the Port of Los Angeles on August 25, 2003, one of 11,000 arriving at the port that day. The suitcase containing the material cleared customs, was stored in an adjacent warehouse, and was delivered to a storage warehouse one mile from the Los Angeles Convention Center (Allison, 2004: 104-105).
- To demonstrate that the first event was not a fluke, on August 23, 2003, one year after the original episode, ABC News transported the same 15-pound device from Jakarta, Indonesia in a cargo container to the Port of Los Angeles. It was again inspected by Customs, and again allowed to be trucked to the downtown warehouse (Ervin, 2006, pp118-119).
- Less than a month after September 11, 2001, an Egyptian Al Qaeda suspect was found hidden in a container on its way from Egypt to Toronto. He had with him a laptop computer, a satellite phone, airport maps, three security badges for airports in Canada, Egypt, and Thailand, and a certificate from a two-year course in airplane engine maintenance. He even had a bed and a bathroom.
- In January, 2005, 39 Chinese stowaways managed to send themselves from Shekou, China, by way of Hong Kong, inside two containers, and to be put in storage in a U.S. port. They were only detected, by a crane operator, when they attempted to climb over a fence.
- Earlier this year, 21 Chinese from Shanghai infiltrated the Port of Seattle in a container. Their container was identified by the Coast Guard for further investigation, but was left overnight because of insufficient personnel. The stowaways were discovered, by a crane operator, because they all were wearing suits.
- Four years ago, three Palestinian terrorists hid themselves and a large cache of arms inside a shipping container with a false back and had themselves shipped into Israel, undetected. Once inside Israel, the three sneaked out of the container and killed several local residents.

Consequences. A number of studies have estimated that a nuclear bomb, a "dirty bomb," or a radiological and biological device could cause considerable damage and could kill and/or contaminate thousands of citizens within several miles of a port (Loveless, et al., 2003). Ironically, however, "the cost of our response could be far more economically damaging than the attack itself" (Loveless, 2003, p.2). Absent appropriate security measures, the Hart-Rudman report points to the considerable risk that:

> Should the maritime or surface elements of America's global transportation system be used as a weapon delivery device, the response right now would almost certainly be to

> shut the system down at an enormous cost to the economies of the United States and its trade partners....bringing the global container industry to its knees.

Customs Commissioner Robert Bonner (2002) made the same point:

> If terrorists used a sea container to conceal a weapon of mass destruction and detonated it on arrival at a port, the impact on global trade and the global economy could be immediate and devastating—all nations would be affected. No container ships would be allowed to unload at U.S. ports after such an incident.

Exploding or ramming a massive oil, LPG, or LNG tanker in a congested urban environment also could cause thousands of casualties and produce enormous environmental damage.

The U.S. Navy has considerable assets stationed in or near several American ports, most notably Norfolk, Virginia and San Diego, California. Although the Navy has primary responsibility for protecting these ships, other port interests also have concerns about the possibility of terrorists damaging or sinking one of these vessels, particularly those that are nuclear-powered.

Finally, 17 ports have been designated "strategic" by the Department of Defense and the Department of Transportation.[12] They are so designated because in the event of a large-scale military deployment, DOD would transport more than ninety-five percent of all equipment and supplies needed for military operations by sea. These ports are therefore vital to national security. If the strategic ports (or the ships carrying military supplies) were attacked, not only could massive civilian casualties result, but also valuable cargo and time could be lost, as military mobilization would be forced to rely on already overburdened airlift resources.

National/International Developments: Broad Policy Measures to Address Port Security

For most of the maritime industry's history, "security" concerns could be epitomized by scenes from *On the Waterfront*, in which longshoremen took merchandise from shipping pallets at will, either for their own use or for resale. Theft from cargo was considered part of the cost of doing business, and in some quarters was considered one of the "perks" of employment at our ports. That era began to fade on April 26, 1956, when 58 aluminum truck bodies were shipped from Newark, New Jersey to Houston, Texas. This meager shipment represented the beginning of the "container revolution," a complete transformation of the shipping industry. The enclosure of cargo within 20-foot containers made shipping much less expensive, transformed the life of seaport workers, and created a change in the concept of "port security." As Levinson (2006: 6) points out in his history of this transformation:

[12] Thirteen of these ports are commercial ports, three are military ammunition ports, and one is a military port (U.S. Government General Accounting Office, 2002b, p 5).

> Containers can be just as efficient for smuggling undeclared merchandise, illegal drugs, undocumented immigrants, and terrorist bombs as for moving legitimate cargo.

Alarms about security on cruise ships were raised in October 1985, when four members of the Palestinian Liberation Front hijacked the passenger liner *Achille Lauro* off the coast of Egypt, demanding the release of 50 Palestinian prisoners held by Israel. Wheelchair-bound Leon Klinghoffer, a Jewish American, was thrown overboard during a two-day seizure. The vulnerability of such ships, and the consequences of the fear created by the seizure, became of great concern to the cruise industry, which increased security precautions on its vessels. Recognizing the seriousness of the issue of maritime security, the federal government has taken several important policy steps--both before and after September 11. These broad policy changes are important and set the context for our sites visits, for these measures have had an impact on all ports in the United States, including those seen by PERF researchers during our site visits.

Pre-September 11th Port Security Measures

Before the September 11th attacks, port security focused on physical security and access control, cargo security, passenger and crew security, and military mobilization security, and was oriented toward crime-related activities. Although the maritime community acknowledged the threat of terrorism, very few specific security measures were taken to deter or undermine a maritime terrorist threat. Despite this general neglect, the U.S. government in the late 1990s had initiated several efforts regarding protection of the ports. The Public Policy Institute of California (Haveman and Shatz, 2006: 186)[13] recently outlined the pre-September 11th steps taken in the area of port security by the federal government. Below we outline those steps.

In 1984, the U.S. Maritime Administration (MARAD) signed a Memorandum of Understanding with the U.S. Army Corps of Engineers, the U.S. Coast Guard, the Military Traffic Management Command, the Military Sealift Command, the U.S. Joint Forces Command, the U.S. Transportation Command, the Maritime Defense Zone, and the U.S. Forces Command to establish the National Port Readiness Network. This Network was created to ensure that commercial ports designated as "strategic" would remain ready to support force deployment during military contingencies and defense emergencies. Also in 1984, the Coast Guard and the Navy created the Maritime Defense Zone, a combined USCG-USN command given the task of maritime defense of the United States. Ports, particularly "strategic ports," were given a high priority in defensive planning in recognition of the infrastructure necessary to load-out military supplies. Ports and outload operations were placed under Navy-Coast Guard "Sub-Sector" commands that effectively combined defensive operations between the services by co-locating Coast Guard and Navy personnel in operations centers that would oversee all military operations within the port during times of national emergency.

The 1990s included additional activities to secure the nation's ports. In early 1990, the Maritime Administration (MARAD) conducted sessions on maritime terrorism and drug interdiction in the Ports of New York, Los Angeles/Long Beach, New Orleans, and Philadelphia. Shortly thereafter, MARAD also developed a maritime and terrorism course for the Federal Law Enforcement Training Center (FLETC) in Glenco, Georgia. In late 1993, the U.S. Congress

[13] Haveman, Jon, D. and Howard J. Shatz (2006). Protecting the Nation's Seaports: Balancing Security and Cost. Public Policy Institute of California: San Francisco, CA.

enacted the Customs Modernization Act, calling for "shared responsibility" between the Treasury Department's Bureau of Customs and the private sector, specifically importers. The act states that both public- and private-sector participants have equal roles to play in ensuring compliance with trade and customs laws, and legally shifted the responsibility for merchandise declarations to the importer. Starting in 1995, MARAD began conducting training sessions for port authorities on bomb threats to determine best practices and capabilities of various government agencies and bomb squads. In 1997, the Department of Transportation, with the assistance of MARAD, released two security guides (*Port Security: A National Planning Guide* and *Port Security: Security Force Management).* These guides provided local governments and the commercial maritime industry with a common basis upon which to establish port security standards and the outcomes expected from meeting those standards. In 1998, Congress directed the creation of a Marine Transportation System (MTS) Task Force to assess the capabilities and vulnerabilities of that system. MTS incorporated the work of a large number of agencies connected with the maritime sector, including the U.S. Coast Guard, the U.S. Army, the National Oceanic and Atmospheric Administration (NOAA), the U.S. MARAD, and the Environmental Protection Agency (EPA). The original impetus for the MTS was operational in nature. There was a sense that the system's infrastructure was aging and not likely capable of supporting the expected increase in maritime activities. While not the exclusive focus of the MTS Initiative, port security was a core element. Although the task force passed off major responsibility for considerations of maritime security to the Interagency Commission on Crime and Security in U.S. Seaports (discussed below), the MTS report (Department of Transportation, 1999: 88-91) did identify five strategic areas for action related to security of the maritime transportation system: Improve security awareness, improve transparency, ensure qualified operators, forge stronger public/private partnerships, and strengthen international cooperation.

In early 1999, President Bill Clinton directed the Secretary of the Treasury, the Secretary of Transportation, and the Attorney General to establish the Interagency Commission on Crime and Security in U.S. Seaports to examine the threats of crime and terrorism in America's seaports. This commission produced *Report of the Interagency Commission on Crime and Security in U.S. Seaports*, identifying the need to move security efforts beyond U.S. borders. The commission report (2000) provided:

- An analysis of the nature and extent of serious crime and an assessment of the overall state of security in U.S. seaports;
- An overview of the specific missions and authorities of federal agencies with relevant responsibilities, together with a description in general terms of the typical roles played by state and local agencies as well as by the private sector;
- An assessment of the nature and effectiveness of the ongoing coordination among the federal, state, and local government agencies; and
- Recommendations for improving the response of the federal, state, and local governments to the problem of seaport crime and security. The report (2000: 73) assessed security at 12 American seaports and, after a thorough risk assessment, concluded that, "The threat of terrorism is low, but the vulnerability of seaports to terrorism is high."

In the new millennium, pre-September 11th, there was also the attack by suicide bombers on the guided-missile destroyer U.S.S. *Cole* in the Yemen port of Aden on October 12, 2000, which killed 17 sailors. This incident further heightened attention to the attractiveness of

maritime targets to terrorists. The Navy immediately intensified its security precautions around its ships.

Thus, although international and national authorities were not highly active in addressing the issue of maritime or port security before 9/11, they were not totally quiescent either. As described in a summary assessment provided by Haveman and Shatz (2006: 190):

> … even before the summer of 2001, a number of ideas for improving seaport security had been proposed. These included developing port security plans, developing new methods of tracking cargo, pushing the borders of the United States out and sealing the supply chain, designating a lead agency for port security, and using public-private partnerships to carry out some of these tasks.

The attacks on September 11, 2001, to paraphrase Samuel Johnson, "concentrated the minds of policy makers wonderfully" on the vulnerability of all modes of transportation and commerce. In immediate response, as mentioned above, all seaports were closed for several days. The Coast Guard dispatched ships to provide security at all major American ports.

Post-September 11th Port Security Measures

An excellent description of the various federal efforts to enhance seaport security has been set forth by the Public Policy Institute of California report (Haveman and Shatz, 2006: 190). Haveman and Shatz (2006) divide the federal efforts into five related categories: (1) planning for protection, response, and recovery; (2) hardening ports to make them less-attractive targets; (3) sealing gaps in international supply chains—the points where terrorists, their supplies, or their weapons could enter shipping channels; (4) identifying and closing security weaknesses outside the United States, preferably in foreign countries before the goods start their journey here; and (5) upgrading technologies to accomplish the first four tasks. These federal initiatives attempt to achieve the aims of identifying and reducing the vulnerabilities of port facilities and of the vessels in seaports; securing the cargo flowing through seaports; and enhancing awareness of the entire global maritime environment (Wrightson, 2005).[14]

To achieve these aims, there are numerous federal programs and initiatives that create overlapping "layers of security." The Department of Homeland Security concept of "layers of security" involves multiple types of activities to create a network of interdependent, overlapping and purposefully redundant checkpoints designed to reduce vulnerabilities, as well as to detect, deter and defeat threats (Wrightson, 2005), covering the various components of the maritime transportation system (e.g., people, infrastructure, conveyances and information systems). For example, at the Port of Seattle our research team observed on our site visit a layered approach to security that included:

- Screening all foreign vessels prior to arrival: 96-Hour Advance Notice of Arrival
- Boarding of designated High Interest Vessels (HIVs) before they enter port
- High Value Assets (HVA)/High Value Unit (HVU) escorts
- High Capacity Passenger Vessel escorts of cruise ships and ferries
- Increased harbor patrol and surveillance of critical infrastructure
- Carry out Security Zones, Restricted Areas, Naval Force Protection Zones

[14] Wrightson, Margaret T., "Maritime Security: Enhancements Made, But Implementation and Sustainability Remain Key Challenges," Testimony Before the Committee on Commerce, Science, and Transportation, U.S. Senate, GAO-05-448T, U.S. Government Accountability Office, Washington, D.C., May 17, 2005.

- Increased security for naval assets and facilities

There have been a number of key policy measures that have been established to enhance the security of the nation's ports, including: the Maritime Transportation Security Act of 2002 (MTSA), the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT), the National Targeting Center (NTC), port security grant programs, the expanded programs of the Coast Guard, and a number of other key federal initiatives.

Maritime Transportation Security Act of 2002 (MTSA). The MTSA was enacted by the U.S. Congress, and then signed by President Bush on November 25, 2002. This law provides the overall planning and response framework to port security for the nation. MTSA sets out broad guidelines for securing the nation's ports and related intermodal facilities. Tasked with implementing many of the MTSA measures, the U.S. Coast Guard has become the lead agency in maritime and port security. The Coast Guard is also responsible for overseeing for the United States the implementation of the International Ship and Port Facility Security (ISPS) Code, a set of measures that broaden maritime security planning and preparedness to the whole world and that were developed by the International Maritime Organization (IMO).

Since the passage of the MTSA, there has been other supporting legislation. For example, in December 2004 Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004, which generally imposes a sense of urgency on DHS to strengthen maritime security by imposing deadlines on the agency in planning and carrying out certain maritime security activities called for in MTSA.

Nevertheless, the MTSA is very comprehensive in its requirements. Among the key features of the MTSA are the following:

- Requirements for port, facility, and vessel vulnerability assessments.
- Preparation by the Secretary of Transportation of a National Maritime Transportation Security Plan and Area Plans for each U.S. Coast Guard Captain of the Port Zone.
- Development of security plans for certain facilities and commercial vessels.
- The issuance and use of Transportation Security Cards [later called Transportation Worker Identification Credentials (TWIC)] for personnel whose responsibilities require them to access secure spaces aboard ships and ports.
- Establishment of a permanent program of grants to facilitate the enhancement of maritime security.
- Assessment by the Secretary of Transportation of the effectiveness of antiterrorism measures at foreign ports.
- Establishment of an enhanced system of foreign seafarer identification.
- Creation of Maritime Security Advisory Committees at national and area levels.
- Installation and operation of automatic identification systems aboard certain commercial vessels.
- Establishment of a program to better secure international intermodal transportation systems, to include cargo screening, tracking, physical security, compliance monitoring, and related issues.
- Provision of civil penalties for violation of statutes or regulations.
- Extension of seaward jurisdiction of the Espionage Act of 1917 to 12 nautical miles offshore of the territorial sea baseline.
- Codification of the U.S. Coast Guard Sea Marshal program and consideration of utilizing merchant mariners and other personnel to assist the Coast Guard.

- Requirements that shipment data be provided electronically to U.S. Customs prior to arrival or departure of cargo.
- Reporting by the Secretary of Transportation to Congress on foreign-flag vessels calling at United States ports.
- Development of standards and curriculum for maritime security professional training.

Container Security Initiative (CSI). The CSI is an overseas program announced in January 2002, operated by U.S. Customs and Border Protection (CBP), that helps build awareness and enhances terrorism prevention measures. CSI addresses the threats to the United States and global trade posed by the possible use of a maritime container to deliver a nuclear or other weapon. CSI is designed to ensure that all containers that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels and arrive at a U.S. port. CBP has multidisciplinary teams of U.S. officers from both CBP and Immigration and Customs Enforcement (ICE) stationed overseas to work cooperatively with their foreign government counterparts. These officers target and prescreen containers and investigate leads related to terrorist threats to cargo. A core element of CSI is using "smarter," "tamper evident" containers that will better secure containerized shipping. This "Smart Box Initiative" couples an internationally approved mechanical seal affixed to an alternate location on containers with an electronic container security device designed to deter and detect tampering of the container door. If someone attempts to open the cargo door after it has been sealed, the "smart box" device will reflect that there has been an attempted intrusion. The four core elements of CSI are the following (see www.cbp.gov/xp/cgov/border_security/ international_ activities/csi):

- *Identify high-risk containers*: CBP uses automated targeting tools to identify containers that pose a potential risk for terrorism, based on advance information and strategic intelligence[15];
- *Prescreen and evaluate containers before they are shipped*: Containers are screened as early in the supply chain as possible, generally at the port of departure;
- *Use technology to prescreen high-risk containers without slowing down the movement of trade*: This technology includes large-scale X-ray and gamma ray machines and radiation detection devices[16]; and
- *Use smarter, more secure containers*: These containers will allow CBP officers at U.S. ports of arrival to identify containers that have been tampered with during transit.

CSI has the cooperation of 26 customs administrations that have committed to joining CSI and are at various stages of implementation. CSI is now operational at ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America. Most of the top

[15] In 2003, the U.S. Department of Energy developed a somewhat similar effort to screen cargo. Referred to as the Megaports Initiative, this is a program to screen containerized cargo as it moves through the global maritime shipping network for nuclear and other radiological materials. To accomplish this goal, the program provides and installs Radiation Detection Systems (hardware, software, and communications) at several high-volume international seaports.

[16] CBP has installed various types of radiation detection devices at various ports throughout the United States. There are three types of these devices: Radiation Isotope Identifier Devices (RIIDs), Radiation Portal Monitors (RPMs), and Personal Radiation Detectors (PRDs).

20 ports have agreed to join CSI and are at various stages of implementation. These 20 ports account for approximately 66 percent of sea containers shipped to the United States. CSI operational seaports include: Rotterdam, LeHavre, Bremerhaven, Hamburg, Antwerp, Singapore, Yokohama, Tokyo, Hong Kong, Göteborg, Felixstowe, Genoa, La Spezia, Busan, Durban, Vancouver, Montreal, Halifax and Port Klang. It should be pointed out that this program has been subjected to criticism (see, particularly, GAO [2005] and Erwin [2006]).

Customs-Trade Partnership Against Terrorism (C-TPAT). In November 2001, CBP announced the creation of the C-TPAT program. C-TPAT aims at getting companies that are involved in the movement of goods to seal their supply chains. This effort is a public-private partnership aimed at securing the supply chain from point of origin through entry into the United States. Similar to other Department of Homeland Security programs, such as Known Shipper, Registered Traveler, and Free and Secure Trade (FAST), C-TPAT provides expedited clearance to shippers who volunteer to undergo a security check and are determined by such a check to be low-risk. The theory is that such programs allow necessarily limited resources to be concentrated on those persons or products that are likely to be high-risk. Members of the program include U.S. importers, customs brokers, terminal operators, carriers, and foreign manufacturers. Members voluntarily agree to take steps to secure their part of the supply chain in exchange for fewer physical inspections and a less extensive document review.[17]

National Targeting Center (NTC). Working through a local U.S. Customs and Border Protection office, another reported resource used by our participating research sites is the NTC. In particular, ports with developed intelligence-gathering capabilities (e.g., Port of Charleston through project SeaHawk) have found the NTC a valuable resource. The NTC was established in October 21, 2001 in direct response to the terrorist attacks of 9/11. Since then it has become the main anti-terrorism facility for DHS. The Center, originally staffed exclusively by former U.S. Customs Service personnel, now has integrated personnel from all DHS disciplines and has established liaison with the U.S. Coast Guard, the Transportation Security Administration, the Department of Energy, and U.S. Immigration and Customs Enforcement. The FBI also has representatives on site from their Counterterrorism Watch (CT Watch) program, which is the central point within the Bureau for gathering and managing domestic and international terrorism threats. The Food and Drug Administration's Prior Notice Center is also a part of the center.

The NTC is designed to not only assist seaports with their prevention efforts, but also provide information useful for responding to any incident of terrorism. The priority mission of NTC is to provide tactical targeting and analytical research support for CBP anti-terrorism efforts. Experts in passenger and cargo targeting at the NTC operate around the clock using tools like the Automated Targeting System (ATS) to identify tactical targets and support intra-departmental and inter-agency anti-terrorist operations. In addition to the Automated Targeting System, center personnel have access to the Treasury Enforcement Communications System (TECS), the Automated Commercial System (ACS), and the Automated Entry System (AES). The NTC also supports maritime operations including the Container Security Initiative (CSI) with personnel stationed at critical foreign ports throughout the world.

Port Security Grant programs. Implementing the federal initiatives and programs described above poses a significant financial burden for the ports and the companies that operate port facilities. The federal grants program is designed to help with some of this burden by providing for federal assistance. However, it should be pointed out that the cost of MTSA

[17] A number of critiques have been leveled against this program, particularly by the Government Accountability Office (2003, 2005a) and Ervin (2006).

compliance is over $7 billion over a 10-year period (according to U.S. Coast Guard estimates). As of September 2005, the federal government had provided about $780 million in federal port-related grants. Five rounds of Port Security Grants have been awarded, initially under the auspices of the U.S. Maritime Administration and more recently the Transportation Security Administration. TSA has been charged with managing a competitive process and distributing $93 million to critical national seaports to offset costs for various facility and operational security enhancements. Grants were awarded to conduct security assessments and develop strategies to fill security gaps, to enhance facility and operational security, and to fund demonstration projects to explore the use of new security technologies. In later years, after the development of a TSA vulnerability self-assessment tool, TSA provided grants focused on enhanced facility and operational security (Haveman and Shatz, 2006: 203-204). In selecting grantees, federal officials have tended to give preference to single-terminal or facility-specific projects rather than to port-wide projects (Haveman and Shatz, 2006: 203-204). However, projects that enhance intermodal transportation security within the port environment have also been given preference (Haveman and Shatz, 2006: 203-204). The TSA and DHS have preferred projects that address access, command, control, coordination and communication, and physical security, and have also emphasized projects that focus on prevention, deterrence, and detection rather than consequence management (Haveman and Shatz, 2006: 203-204).

While there has been controversy and debate around the allocation of port security grants[18], these grants were reported to be helpful by our participating sites that received them. The mission of the Port Security Grant program is to create a sustainable, risk-based effort for the protection of ports from terrorism. The Port Security Grant program provides federal resources for projects to enhance facility and operational security for critical national seaports. Port officials use the funds to analyze vulnerabilities and then close gaps in security through physical enhancements like access control gates, fencing, lighting, and advanced communication and surveillance systems. The program also funds the implementation of security strategies to respond to terror threats. The Port Security Grant program has awarded funds to owners and operators of ports, terminals, U.S. inspected passenger vessels and ferries, as well as port authorities and state and local agencies to improve security for operators and passengers through physical security enhancements.

Port officials have discussed with our team the benefits of these grants and how they have improved their capacity to respond to a terrorist attack. For example, in 2002, the Department of Transportation awarded the Ports of Seattle, Tacoma and Everett a combined $4,769,724 to increase security, including:

- $839,121 for detailed security assessments and mitigation strategies (Seattle - $409,809, Tacoma - $283,372, Everett - $145,940);
- $1,709,601 for surveillance systems at Seattle ($1,150,859) and Tacoma ($558,742);
- $2,163,854 for access controls at Seattle ($1,453,717) and Tacoma ($710,137); and
- Portable gatehouses at Port of Tacoma ($57,148).

In 2003, the Port of Tacoma received grant funding from the Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) for two major port security initiatives - Round II of the TSA Port Security Grant program and Operation Safe Commerce (OSC):

[18] A critique of the first four rounds of funding, conducted by the DHS Inspector General, is provided in Skinner (2005).

- Port of Tacoma perimeter security enhancements, $564,000;
- Port of Tacoma lighting and warning sign improvements, $47,000; and
- OSC supply chain tests for the Tacoma/Seattle Load Center totaling $10.6 million for project team funding and $2.7 million for project management, analysis and evaluation.

In 2004, the Port received funding from the Department of Homeland Security that was to be used for the following improvements:

- Perimeter lighting/physical enhancements at Blair Terminal, $219,150; and
- Perimeter fencing and gate enhancements at Washington United Terminal, $584,664.

While much controversy has surrounded the distribution of these grants and the amounts clearly fall far below the reported billions of dollars necessary to implement the MTSA, they have nevertheless been useful for the ports receiving them. The port officials we talked with would like to see a more streamlined application process and an expansion of the federal grant programs for port security.

Coast Guard. Also clearly connected to port security is the work of the Coast Guard. The Coast Guard routinely inspects and assesses the security of 3,200 regulated facilities in more than 360 U.S. ports at least annually in accordance with the MTSA and the Ports and Waterways Safety Act (PWSA). While the port agencies are responsible for securing their dockyards and facilities, the Coast Guard is responsible for protecting ships, harbors and shorelines. The Coast Guard is charged with assessing the security status of each port and related facilities and suggesting steps needed to improve them. (However, the port needs to absorb the cost of making those improvements). Since 9/11 the Coast Guard has increased its patrols and surveillance for terrorism, many of which were already in place before 9/11. Before the terrorist attacks, the Coast Guard's primary mission was search-and-rescue, intercepting drug smugglers, breaking ice in polar seas, maintaining navigational aids, and enforcing safety regulations. After 9/11, port security is the top priority. Of concern is that despite this new priority, the Coast Guard budget has not seen corresponding budget and staffing increases.

Since 9/11, the Coast Guard has instituted a number of initiatives to enhance port security. To meet MTSA requirements, the Coast Guard has led efforts to conduct seaport-wide security assessments and security plans for each of the nation's seaports. 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.

Separate from MTSA requirements, the Coast Guard established the Port Security Assessment Program to assess vulnerabilities of the nation's 55 most strategic commercial and military seaports. This program is aimed at increasing the information and best practices available to port officials across the country to help them make decisions about how to reduce the vulnerability of their ports. This program has changed considerably since its inception in the days immediately following the September 11 attacks. Among these changes, the Coast Guard has added a new feature—a geographic information system (GIS). The Coast Guard has created a system to display key port information in an electronic geospatially-referenced format to serve as a database that can be easily searched for national, regional and local information. If, for example, a port received notice of potential threats to chemical plants in the area, a well-designed GIS could identify locations of these plants, provide a variety of information about them, and pinpoint available surveillance and response resources for Coast Guard personnel and others involved in port security. This tool is intended to provide up-to-date, readily accessible information to help develop security plans and respond.

In collaboration with the U.S. Navy and other agencies, the Coast Guard has developed an initiative called Maritime Domain Awareness (MDA), aimed at the collection, fusion, and dissemination of intelligence and other information drawn from U.S. joint forces, U.S. government agencies, international coalition partners and forces, and commercial entities. The goal is to combine this information in order to create a comprehensive common operating picture (COP) that would be distributed among users with access to data that is appropriately classified.

The Coast Guard's intelligence branch is also undergoing unprecedented changes. Under the 2002 Fiscal Intelligence Act, the Coast Guard was inducted into the U.S. Intelligence Community, the 14 foreign intelligence agencies and organizations that report to the Director of Central Intelligence. The Coast Guard has increased the number of personnel dedicated to intelligence gathering and has added equipment, systems and facilities to improve its intelligence capabilities (see www.intelligence.gov/1-members_coastguard.shtml). Since 2003, the Coast Guard has started two facilities it calls "Maritime Intelligence Fusion Centers" that provide 24/7 watch over maritime traffic and developments. The Maritime Intelligence Fusion Centers are located in Norfolk, Va., and Alameda, Calif. The fusion centers were created to serve partly as a collection and distribution point for all Coast Guard-gathered maritime intelligence and to monitor areas of interest, track events, follow vessels of interest, provide analysis and evaluate trends (see www.uscg.mil/lantarea/mifclant/index.htm). Recipients can include nearly everyone in the Coast Guard chain of command, from the President and DHS Secretary to the commandant, area commanders, district offices, ship operators, maritime safety offices, port security personnel and air crews (see www.uscg.mil/lantarea/mifclant/index.htm). The two fusion centers provide information to operational units, but also work in concert with the Coast Guard Intelligence Coordination Center (ICC) at the National Maritime Intelligence Center in Suitland, Md. (see www.uscg.mil/lantarea/mifclant/index.htm). The ICC is responsible for producing and disseminating intelligence with a Coast Guard perspective and providing ready access to this intelligence to those responsible for the nation's maritime domain awareness (see www.uscg.mil/lantarea/mifclant/index.htm). Co-located with the Navy and other agencies, it also provides quick access to others responsible for the nation's maritime awareness.

The Coast Guard has also created Field Intelligence Support Teams (FISTs) to conduct initial analysis of intelligence in coordination with federal, state, and local law enforcement and intelligence agencies. The FISTs also provide tactical law enforcement intelligence support to Captains of the Port and other ranking officials; provide program oversight and support to the Sector Intelligence Officers and Command Intelligence Officers; facilitate liaisons with federal, state and local partners; and actively identify and pursue intelligence collection and analysis.

Additionally, the Coast Guard has increased its number of high-interest vessel boardings since 9/11 (see www.nationaldefensemagazine.org/issues/2003/Jun/ US_Coast_Guard.htm). Before they are allowed to enter port, all incoming vessels to the United States are screened for the security risk they pose based on information about the vessel's cargo, size, voyage, security history and any intelligence information. Those identified as higher risk are targeted for an offshore boarding to ensure potential security issues are addressed prior to entry into the port (see www.nationaldefensemagazine.org/issues/2003/Jun/ US_Coast_Guard.htm). In addition, the Coast Guard randomly selects vessels for security boardings to ensure an element of unpredictability and deterrence. Specially trained Coast Guard teams board the boats through traditional water-based methods or via fast roping from helicopters. As part of Operation Port Shield (OPS), the Coast Guard boards every vessel, at sea or at the dock, on its first visit to a

U.S. port to ensure that the vessel is complaint with U.S. security standards (see www.d8externalaffairs.com/go/doc/425/41878/).

Another resource for local seaports is the Coast Guard's Maritime Safety and Security Teams (MSSTs). MSSTs are a Coast Guard rapid response force assigned to vital ports and capable of nationwide deployment via air, ground or sea transportation to meet emerging threats. MSSTs were created in direct response to the terrorist attacks on Sept. 11, 2001. They have unique capabilities, including explosive-detection dogs, personnel trained to conduct fast-roping deployments from a helicopter to a hostile vessel, and anti-terrorism/force protection. MSST personnel receive training in Advanced Tactical Boat Operations and Anti-Terrorism/Force Protection at the Special Missions Training Center located at Camp Lejeune , N.C.

The Port of Seattle was the first port in the nation to get an MSST stationed at its port. In our discussions with officials of the Port of Seattle, they discussed how their MSST has served as an important force multiplier that enhanced their security capabilities during major marine events, contingencies, and other port-level operations. MSSTs have been used as force multipliers at the Port of Seattle because they possess maritime law enforcement expertise and authority with lethal and non-lethal use of force. Also, with machine guns mounted in high-speed boats, Seattle port officials view the MSSTs as a deterrent to terrorists.

MSST is modeled after the Port Security Unit (PSU) and Law Enforcement Detachment (LEDET) programs. MSSTs provide a complementary non-redundant capability designed to close critical security gaps in our nation's strategic seaports. MSSTs are staffed to support continuous law enforcement operations both ashore and afloat. Four teams were established in 2002 (Seattle; Chesapeake, VA; Los Angeles/Long Beach; and Houston/Galveston). Additional teams were established in 2003 (San Francisco; Ft. Wadsworth, NY; St. Marys, GA.; and Boston); two teams were added in 2004 (Anchorage and New Orleans); and three more in 2005 (Miami, Honolulu, and San Diego). Each MSST has about 75 active-duty personnel. Each MSST unit has six trailerable boats, making them capable of deploying by ground, air and sea. They also have three Physical Security Teams along with two canine handling teams. The MSSTs are able to augment local Sea Marshal operations with their unique training and capabilities. Each unit consists of two teams which can be deployed separately or together and are capable of being deployed within 12 hours of notification and can be operationally ready within four hours upon arrival in any given port.

As required by the MTSA, the Coast Guard has created and supervises Area Maritime Security Committees (AMSCs), which serve as forums for local seaport stakeholders from federal agencies, state and local government, law enforcement, and private industries to gain a comprehensive perspective of security issues at the nation's seaports. 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.

The Coast Guard has also participated in the creation of Interagency Operational Centers, which serve as the central location for representatives of various federal and nonfederal agencies to collect and disseminate information about maritime activities. The centers collect and process information from radar, sensors, and cameras, as well as other data on vessels, cargo, and crew. These centers are operational in nature, unlike the AMSCs, with a unified or joint command structure designed to receive information and act on it.

Another program of the U.S. Coast Guard is a formal assessment program called the Port Vulnerability Assessment (PVA) program. Vulnerability assessments involve identifying and

quantifying vulnerabilities in a system. The system being studied could be a physical facility (e.g., a shipyard) or a larger system (e.g., a communications infrastructure for a seaport). All of the sites we visited engaged to some degree in conducting vulnerability assessments. Most of these assessments included functional assessments of structural protection, physical security, communications, emergency preparedness, fire protection and prevention, utilities protection, information assurance, and other port-specific systems.

Two of our participating sites (the Ports of Savannah and Charleston) have engaged in the PVA program, and the other sites that our team visited regularly engage in other forms of vulnerability assessments. The purpose to PVA is to: (1) Gauge the susceptibility of maritime critical infrastructure to negative consequences from intentional acts, accidents, and natural disasters; (2) make appropriate port stakeholders aware of these vulnerabilities; and (3) recommend mitigation strategies to protect the public, the environment, and U.S. economic interests as required for national security. Ports that are interested in improving their approach to vulnerability assessments should consult with their local Coast Guard and consider linking with the PVA program.

Once vulnerability assessments are completed, this information is used to develop a Facility Security Plan (FSP). Every regulated U.S. port facility, regardless of owner/operator, is required to establish and implement a comprehensive FSP that specifically addresses the vulnerabilities identified in the facility security assessment. This includes detailing measures and procedures for controlling access to the facility, such as screening; designating employees with key security responsibilities; verifying credentials of port workers; inspecting cargo for tampering; designating security responsibilities; engaging in quarterly training, drills and annual exercises; and reporting of all breaches of security or suspicious activity, among other security measures. On our site visits we generally observed strong working relationships between local port authorities and the U.S. Coast Guard on developing FSPs. The Coast Guard regularly reviews, approves, assesses and inspects these plans and facilities to ensure compliance.

In accordance with MTSA, the Coast Guard (according to its website) has completed verification of security plans for U.S. ports and facilities and vessels operating in U.S. waters. Specifically:

- Port Threat Assessments for all 55 militarily or economically critical ports have been completed. The Coast Guard has developed 44 Area Maritime Security Plans covering 361 ports, the Great Lakes, the Inland and Western Rivers, and the Outer Continental Shelf region.
- The Coast Guard completed initial security plan verification exams on all 6,200 U.S.-flag inspected vessels on July 1, 2005.
- The Coast Guard has completed verification examinations on uninspected vessels regulated under the MTSA.
- Reviewed and approved 3,200 facility security plans.
- Approved 60 offshore facility security plans.

Port officials from Seattle talked to our research team about the benefits of helping federal law enforcement in a program called “Operation Drydock.” These officials raised their level of awareness of the complexity of the security problems facing seaports based on the experience of Operation Drydock. The Coast Guard initiated Operation Drydock in December 2002 as a comprehensive criminal and counterterrorism investigation designed to identify vulnerabilities in the merchant mariner credentialing process. The Coast Guard, working with the

FBI's National Joint Terrorism Task Forces (NJTTF) and other interagency partners, compares the names of over 220,000 credentialed merchant mariners against law enforcement information to identify anomalies. Operation Drydock revealed nine individuals who held credentials and had suspected associations with terrorist groups. In Seattle, a U.S. merchant mariner was sentenced to two months in custody, followed by up to 60 days in a halfway house as well as two years of supervised release, for falsely claiming that he had never been convicted of a criminal offense on his application for a Merchant Mariner license submitted to the U.S. Coast Guard in Seattle in January, 2001. This case marked the first time a merchant mariner was convicted of a criminal offense of this type at trial. Merchant mariner credentials are often used as an identification document that allows mariners to come and go from the ship while it is docked in a foreign port. This investigation led to enhancements to the criminal background check process for applicants, resulted in increased security features on the cards themselves, and raised awareness of the need to monitor crews of the U.S. merchant fleet.

At the Port of Miami, officials reported on a very useful awareness-raising program called America's Waterway Watch (AWW). AWW is a combined effort of the Coast Guard and its Reserve and Auxiliary components, enlisting the active participation of those who live, work or play around America's waterfront areas. Coast Guard Reserve personnel concentrate on connecting with businesses and government agencies, while Auxiliarists focus on building AWW awareness among the recreational boating public. AWW is a nationwide initiative similar to the well-known and successful Neighborhood Watch program that asks community members to report suspicious activities to local law enforcement agencies. AWW is a public outreach program, encouraging participants to simply report suspicious activity to the Coast Guard and/or other law enforcement agencies or by calling 1-877-24-WATCH. The goal of America's Waterway Watch is to help prevent acts of terrorism and other illegal activity that jeopardizes maritime homeland security by having members of the maritime and recreational boating industries, as well as the boating public, recognize and report to the police suspicious activity that may be an indicator of potential terrorism.

At the Port of Miami, Sayed Abdul Malike, a suspected terrorist with known connections to Al Qaeda, was apprehended in 2003 based upon a tip from a local charter boat captain to AWW. This cruise boat operator reported suspicious activity by Malike, such as videotaping port facilities and asking about the infrastructure of bridges and how close boats could get to bridges and cruise ships, which led to Malike's arrest by the FBI.

Starting in 1996, the USCG began developing an Integrated Deepwater System (known as Deepwater) acquisition program, a long-term plan to replace or modernize its fleet of aircraft and vessels, and to improve its command and control and logistics systems. Before the September 11 attacks, this plan focused on producing or acquiring aircraft and vessels that would function in the Coast Guard's traditional at-sea roles, such as interdicting illicit drug shipments or rescuing mariners having difficulty at sea. After the attacks, however, these aircraft and vessels began to take on additional missions related to the protection of ports, waterways, and coastal areas. An award was announced in June 2002 to Integrated Coast Guard Systems—a partnership between electronics maker Lockheed Martin and shipbuilder Northrop Grumman. The Coast Guard revised the Deepwater implementation plan to provide replacement assets that could better address the new security-related responsibilities. In August

2005, the Coast Guard issued a revised Deepwater implementation plan detailing the assets it planned to modify or acquire. This plan was further updated in February 2006. Numerous reports have surfaced that there are significant problems with the implementation of the program, however, and the Coast Guard is now taking control of the modernization program itself (Merle and Hsu, 2007).

Other key federal initiatives. The overarching framework for United States maritime security policy was established with the signing by President George W. Bush of National Security Presidential Directives 41 and 13 (NSPD 41 and NSPD 13) on December 21, 2004. These directives called for the creation of a Maritime Security Policy Coordinating Committee (MSPCC) to oversee the development of a National Strategy for Maritime Security (NSMS) and eight supporting implementation plans:

- The National Plan to Achieve Maritime Doman Awareness lays the foundation for an effective understanding of anything associated with the maritime domain and for identifying threats, even those that are distant from our shores, as early as possible.
- The Global Maritime Intelligence Integration Plan uses existing capabilities to integrate all available intelligence regarding potential threats to U.S. interests in the maritime domain.
- The Maritime Operational Threat Response Plan aims for a coordinated U.S. government response to threats against the United States and its interests in the maritime domain by establishing roles and responsibilities, which enables the government to respond quickly and decisively.
- The International Outreach Strategy to enhance maritime security provides a framework to coordinate all maritime security initiatives undertaken with foreign governments and international organizations, and solicits international support for enhanced maritime security.
- The Maritime Infrastructure Recovery Plan recommends standardized procedures for restoration of maritime transportation systems following an incident of national significance.
- The Maritime Transportation Systems Security Plan provides strategic recommendations to holistically improve the security of maritime transportation systems.
- The Maritime Commerce Security Plan establishes a comprehensive plan to secure the maritime supply chain.
- The Domestic Outreach Plan engages non-federal input to assist with the development and implementation of maritime security policies resulting from the NSPD 41 and NSPD 13.

Our team observed a number of promising practices in the area of protocols and systems for detecting and monitoring port-related security risks that involve providing real-time information on security risks before the vessel arrives at a U.S. port, including: The 24-hour Advanced Manifest Rule, the Automated Targeting System, the Automatic Identification System, Operation Safe Commerce, the Terrorist Screening Center, and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program. .

The first of these measures, the 24-hour Advanced Manifest Rule, focuses on improving awareness on threats from overseas information sources. The 24-hour Advanced Manifest Rule

requires all sea carriers (with the exception of bulk carriers and approved break bulk cargo) to provide proper cargo descriptions and valid consignee addresses 24 hours before cargo is loaded at the foreign port for shipment to the United States through the Sea Automated Manifest System.[19] While some port officials we talked to about this rule have heard numerous complaints about this new rule from sea carriers, they felt on balance this rule will enhance security at their ports. Failure to meet the 24-hour Advanced Manifest Rule results in a "do not load" message and other penalties. This rule has helped increase awareness of what is being loaded onto ships bound for the United States, and the advance information enables ports to evaluate the terrorist risk from sea containers.

Related to this rule is the 96-Hour Advance Notice of Arrival for ships in transit to the United States. Ships must notify the Coast Guard 96 hours before arriving in a U.S. port and must provide detailed information on the crew, passengers, cargo, and voyage history. This information is analyzed using databases and intelligence information, including reviewing previous security problems with the vessel or illegal activity on the part of the crew. This analysis will include an assessment of the security environment in previous ports of call. By obtaining this information well in advance of a vessel's arrival, the U.S. Coast Guard is able to make determinations about which vessels require additional attention, including security precautions such as an at-sea boarding or armed escort during transit to and from port. The 24-hour Advanced Manifest Rule was considered helpful at our study sites, with none of them raising any major objections.

Across the ports our research team visited, the Automated Targeting System (ATS) is being used and (along with the 24-Hour Manifest Rule) is enhancing security. ATS is a flexible system that integrates enforcement and commercial databases. It is a targeting tool that helps CBP focus its inspection efforts on high-risk cargo. ATS analyzes electronic data related to individual shipments prior to arrival and ranks them in order of risk, based on the application of algorithms and rules. The scores are divided into thresholds associated with further action by CBP, such as document review and inspection.

The industry data that feeds the ATS is substantial. First, there are data related to the 24-Hour Manifest Rule, which are essential to CBP's targeting success in the sea environment. ATS processes this information, which allows the CBP to evaluate all awaiting containers for terrorist risk before they are loaded and shipped to U.S. seaports. Although advance manifest data is a major component of what is analyzed, ATS also sorts through intelligence and data contained in government law enforcement and trade databases. Advance information is also received on all incoming passengers. ATS processes information, picking up on anomalies and "red flags," and provides a basis for targeters to determine which cargo or passengers are "high risk," whether they require scrutiny at the port of entry or overseas, or whether they can come to U.S. shores at all. For ships in transit, the ATS serves as an important tool for performing transactional risk assessments and evaluating potential port security risks posed by cargo and passengers arriving by sea, air, truck, and rail.

---

[19] Starting in February 2003, CBP began enforcing an Automated Manifest System (AMS) that requires that sea carriers and Non-Vessel Operating Common Carriers (NVOCCs) provide CBP with shipping manifest information 24 hours before a container is loaded for destination in a harbor in the United States.[19] This rule was developed to allow Customs officers to analyze the container content information and identify potential terrorist threats before the U.S.-bound container is loaded at the foreign seaport. Customs is given authority to issue "Do-Not-Load" messages to carriers that violate the rule, instructing that containers may not be loaded on a U.S.-bound ship.

Another part of ATS is Supply Chain Stratified Examination. This examination supplements the ATS by randomly selecting additional containers to be physically examined. The results of the random inspection are compared with those of ATS inspections to improve targeting. Despite its promise, there have been a number of critiques of this program. These critiques may be found in Erwin (2006), GAO (2004), and U.S. Department of Homeland Security Office of Inspector General (2005).

Related to the ATS is the Automatic Identification System (AIS). AIS is a system used by ships and vessel traffic systems, principally for identification of vessels at sea and to avoid collisions. AIS helps to resolve the difficulty of identifying ships when they cannot be physically observed (e.g. at night, in fog, in radar blind arcs or shadows, or at distance), by providing a means for ships to exchange ID, position, course, speed and other ship data with all other nearby ships and ATS stations. It works by integrating a standardized VHF transceiver system with a GPS receiver and other navigational equipment on board ship. AIS is also used to send detailed ship information to other ships and shore-based agencies, allowing for comprehensive, virtually instantaneous vessel tracking and security monitoring. When completed, this system will operate in all navigable waters of the United States.

Next, Operation Safe Commerce (OSC) was launched in November 2002 by the U.S. Department of Transportation (DOT) and the U.S. Customs Service. OSC is a pilot program to identify and analyze security gaps in the present cargo supply chain and to test a number of different products (ranging from cargo information systems to seals, sensors, and tracking devices). OSC has provided three pilot port sites (Los Angeles/Long Beach, New York/New Jersey, and Seattle/Tacoma) with funding to test new security techniques and technologies designed to improve containerized shipping security. We discuss OSC because two of these OSC locations (Los Angeles/Long Beach and Seattle/Tacoma) are research sites in our study, and they identified promising practices associated with OSC. OSC helps build awareness by analyzing security in the commercial supply chain. The technologies tested through the program have the potential to enhance maritime cargo security, protect the global supply chain, and facilitate the flow of commerce. OSC funds business initiatives designed to increase security for container cargo moving throughout the global transportation system. OSC has also served as a test-bed for new security techniques and systems. DOT and Customs have used OSC to identify existing vulnerabilities in the supply chain and develop improved methods for ensuring the security of cargo entering and leaving the United States.

Since the launch of Operation Safe Commerce, the federal government has awarded $58 million as part of the program. One of our participating research sites, the Port of Seattle, has received $27.5 million for nine different projects. Our research team observed elements of OSC in Seattle during our site visit. For example, we observed vehicle-mounted VACIS gamma-ray imaging equipment taking radiographic images of trucks, containers, and other cargo. Our research team had similar positive reports on OSC during our visit to the Los Angeles/Long Beach site.

Another related federal center that can improve port security is the Terrorist Screening Center (TSC). In 2003, the Attorney General, the Secretary of Homeland Security, the Secretary of State, the FBI Director, and the Director of Central Intelligence announced the creation of the TSC. This center was created to consolidate the U.S. government's ability to screen for known and suspected terrorists and to provide for the appropriate and lawful use of terrorist information

in this process.[20] The Center employees use the Terrorist Screening Center Database (TSDB), a compilation of several lists maintained by separate agencies: the Consular Lookout and Support System (CLASS) and TIPOFF file from the Department of State; the Interagency Border and Inspection system (IBIS) from the Department of Homeland Security; the No-Fly and Selectee Lists from the Transportation Security Administration (TSA); the National Automated Immigration Lookout System (NAILS) and the Automated Biometric Identification System (IDENT) from ICE; the Violent Gang and Terrorist Organization File (VGTOF) and the Integrated Automated Fingerprint Identification System (IAFIS) from the FBI; and the Interpol Terrorism Watch List. CBP officers consult this database to screen arriving passengers for customs and immigration violations, and to detect and prevent terrorists and weapons of mass destruction from entering the United States (Department of Homeland Security 2006).

Another related federal effort with the potential to improve port security is the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program. This DHS program, created in 2003, is an automated system to integrate information concerning the entry and exit from the United States of non-immigrant visitors. The program is designed to identify individuals who may (a) pose a threat to the security of the United States, (b) have violated the terms of their admission to the country, or (c) be wanted for the commission of a crime in the United States or elsewhere. The admission into the United States of an individual subject to US-VISIT requirements is contingent upon submission of the information required by the program, including biographical information (name, nationality, and date of birth); biometric data (photographs and digital fingerscans); as well as travel itineraries. This information is used by CBP agents in identifying suspicious persons.

An industry-driven initiative to demonstrate the principles of the OSC, CSI, and C-TPAT is the Smart and Secure Tradelanes (SST) program. SST uses an automated information technology infrastructure to link key international ports with U.S. ports, similar to the Department of Defense Total Asset Visibility network, to improve the tracking and security of inbound shipments by adapting and integrating the most advanced technologies available.

One of the more recent developments in federal legislation to enhance port security is the Security and Accountability for Every Port Act (SAFE). This law was passed and implemented in October 2006. The Act represents a comprehensive reaffirmation and improvement of policies and programs implemented since the attacks of September 11. Among other provisions, this act:

- Codifies the Container Security Initiative (CSI) and the Custom-Trade Partnership Against Terrorism (C-TPAT);
- Directs the creation of interagency operational centers at all 22 high-risk ports;
- Sets an implementation schedule and fee restrictions for the Transportation Worker Identification Credential program (TWIC);
- Mandates the frequency of Coast Guard inspections of maritime facilities, requiring unannounced inspections;
- Requires that all containers entering high-volume U.S. ports be scanned for radiation sources by December 31, 2007;

[20] The TSC was created under the auspices of Homeland Security Presidential Directive 6 (HSPD-6), issued on September 16, 2003.

- Requires the establishment of a Port Security Exercise Program, to test and evaluate the capabilities of various governmental and nongovernmental entities when faced with emergencies, and to improve the communication of lessons learned during the exercises;
- Requires that federal port security grants be awarded on the basis of risk;
- Allows all port facilities within an Area Maritime Transportation Security Plan to apply for such grants;
- Ties port security grants to state plans, area plans, and Port Wide Risk Management plans;
- Requires DHS to deploy nuclear and radiological detection systems at 22 of the nation's largest seaports;
- Calls for the expansion of Coast Guard efforts to work with other countries to assess—and where needed strengthen—their security procedures;
- Mandates that DHS develop a detailed incident recovery plan to get trade moving again in the event of an attack; and
- Supports the creation of cargo scanning pilot programs at overseas ports to test the practicality and effectiveness of systems designed to scan 100 percent of cargo.

Other key international/overseas initiatives. In response to pressure from the United States, the United Nations International Maritime Organization (IMO) moved quickly to promulgate new international requirements to strengthen maritime security. The IMO Maritime Safety Committee developed amendments to the International Convention for the Safety of Life at Sea, 1974 (SOLAS Convention) consisting of measures intended to enhance maritime security, including maritime security education and training. The result was the International Ship and Port Facility Security (ISPS) Code, adopted at a diplomatic conference in London in December 2002, which basically represented an international extension of the Maritime Transportation Security Act (discussed above).

- The ISPS requires passenger and cargo ships of at least 500 gross tons to install a Ship Security Alert System (SSAS) which allows a vessel operator to send a covert alert to shore regarding incidents involving acts of violence, such as piracy or terrorism, indicating the security of the ship is under threat or has been compromised.
- To carry out one of the mandates of the MTSA—to assess the implementation of the International Ship and Port Facility Security Code (ISPS) in nations around the world—the Coast Guard in April 2004 created the International Port Security program (IPSP). The aim of IPSP is to assess the effectiveness of antiterrorism measures in foreign ports, and to protect the global shipping industry by facilitating the implementation of security improvements in ports around the world. IPSP involves teams assembled from experts from the Coast Guard, Customs and Border Protection, and the Transportation Security Administration who visit dozens of ports each year. The IPSP teams evaluate each country's overall compliance with the International Ship and Port Facility Security Code, providing technical assistance as necessary to assist countries with compliance, sharing and aligning best practices in maritime security, and assessing the effectiveness of specific antiterrorism measures in foreign ports.
- The Proliferation Security Initiative (PSI) was launched in July 2003 as a partnership by the United States and several other countries who agreed to

cooperate in detaining and searching ships, aircraft, and vehicles suspected of carrying WMD-related materials as soon as they enter member countries' territory, territorial waters, or airspace. To accommodate international law, bilateral arrangements are made to board vessels and aircraft and/or guide these to participating nations.

- The U.S. Department of Defense has undertaken a counter-proliferation initiative that involves obtaining permission from seafaring countries to allow specially trained U.S. navy boarding teams to conduct inspections of a flag vessel on the seas when there is intelligence that points to the possibility that nuclear material or a weapon may be part of the ship's cargo (Flynn, 2006).

The extent and variety of international and national responses to the problem of maritime security dramatically indicates that the significance of that problem has been widely recognized. While much work still needs to be done, seaports have at least made some strong in-roads into improving security. As outlined in a recent NIJ study (Davis, Ortiz, Rowe, Broz, Rigakos, and Collins, 2006 at http://www.asisonline.org/foundation/noframe/mall.pdf), it appears if the mall security community has made much less progress. Most of the programs and initiatives discussed in this report, however, are general in scope, and not so specific that they only apply to particular individual ports. This report will document the promising practices being implemented by local agencies in our nation's ports.

III. Research Methods

"Promising" Practices Case Study Methodology

Our focus on "best" and most "promising" practices was necessitated by the general lack of research data in the area of port security. While early in this project we considered the use of a national survey on port security, we moved away from that approach. At that point, too little was known about port security to even begin assembling the appropriate questions for a large-scale survey. Instead, we adopted a case study approach to generate a better understanding of the port security landscape. Next, we provide a brief overview of our case study approach, and discuss how we identify "promising" practices.

Case Study Method

We conducted case studies of exemplary and innovative security practices in 17 seaports, with a particular focus on intergovernmental and public-private partnerships and elements of success of those partnerships. The 17 seaports included: San Diego, CA; Los Angeles, CA; Long Beach, CA; Jacksonville, FL; Tampa, FL; Port Lauderdale, FL; Miami, FL; New Orleans, LA; Houston, TX; Galveston, TX; Texas City, TX; Charleston, SC; Savannah, GA; Port of Virginia, VA; Boston, MA; Seattle, WA; and Tacoma, WA.

Case study methods are in-depth, qualitative studies of one or a few illustrative cases (Becker, 1978). According to Yin (1994: 13), a case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident. Also, the case study method, according to Yin (1994:13), copes with the technically distinctive situation in which there will be many more variables than data points, and relies on multiple sources of evidence,

with data needing to converge in a triangulating fashion. The essence of a case study is that it tries to illuminate a decision or set of decisions: why were they taken, how they were implemented, and with what result (Schramm, 1971). Although various research methodologies (e.g., experiments, surveys, and archival analyses) have their strengths and weaknesses, the descriptive case study is the preferred methodology in analyzing the interorganizational relationships in port security. As Yin (1994:7) points out, the case study has a distinct advantage when "…a 'how' or 'why' question is being asked about a contemporary set of events over which the investigator has little or no control."

Given the considerable uncertainty around port security operations and the complexity of the interconnections across the many local, state and federal law enforcement partners involved in providing security, we used an exploratory/descriptive case study methodology. Too little was known about our subject matter to embark on an evaluation of the effects of various port security efforts. The first step is to assemble a rich description of the problem and context for port security and identify key promising practices based on the expert opinion of port personnel. At a later stage, researchers will be in a better position to address some of the questions about the effectiveness of the various security initiatives.

"Promising" Practices

The terms "promising practices" and "best practices" are widely used in many fields; however, there are generally no universally accepted definitions of what constitutes a "best" or a "promising" practice. "Best Practices" is a concept used extensively in industry, management, education and healthcare (for recent reviews and discussion, see Morrison, 2004; Drake, Rosenberg, Teague, Bartels, & Torrey, 2003; Essock, Goldman, Van Tosh et al., 2003; Hermann & Provost, 2003; Lehman, Buchanan, Dickerson, et al., 2003; Silverstein, Wilkniss, & Bloch, 2002). Its basic principle is that a field of study can and should develop consensus about which of many alternative practices are considered the "best" ones within the field or community. The dimensions upon which practices are judged "best" are many, and specific to particular fields and/or applications. Across these fields, best practices generally involve methods or procedures of doing programs, processes, and projects that are exemplary and worth sharing with others. These may be interesting ways of addressing some issue or challenge. Often, they are unique and instructive. Most of the time, they can be shared with others, whose needs are similar enough that the best practice can be taken as one possible way of addressing a similar issue.

In the context of seaport security, there are few evidence-based practices that have been tested scientifically and shown to enhance security. In some ways it is not feasible to use traditional evaluation methods to examine seaport security practices due to the rarity of attacks of any kind on seaports. That is, the traditional "gold standard" of research (the randomized controlled trial) is not a practical approach to assessing the effectiveness of security strategies in seaports. The existing set of port security practices have not been evaluated with rigorous, or even non-rigorous, empirical evaluation methods. Nevertheless, port security officials have had considerable experience with a number of security practices over several (and in some cases many) years. Our report offers their valuable insights into these practices that have been applied in a variety of settings.

In the "Promising Practices" section we use an inclusive approach to deciding if a practice should be included in this report. That is, if the port officials from our study sites suggested that a particular approach was a "promising practice" *and* they could describe how they have implemented it with some success, we included at least some mention of it in the

"Promising Practices" section of this report. We have used a promising practices approach for its instructive value. Believing that the best teacher is experience, we tried to identify the most valuable security practices that have been developed by a range of seaports and share them in a form that can be understood and explored by other ports.

Focus on Promising Local Practices in Port Security

Our study identifies the best and most promising *local* practices in port security. A number of other studies, as outlined in the literature review, have already explored federal wide port security initiatives. Unless there are unique regional variations or compelling local adaptations of a nationwide practice, our study explicitly excluded from our focus programs being implemented by federal agencies, such as the Department of Homeland Security (Coast Guard, Customs and Border Protection, Immigration and Customs Enforcement); or the Department of Justice (Federal Bureau of Investigation; Bureau of Alcohol, Tobacco, Firearms and Explosives).

Confidentiality of Data

Due to the sensitivity of the data we collected and its potential for compromising security at our Nation's ports, we had to limit some of the details we could provide in our descriptions of the local initiatives. It was also necessary, in some cases to neither attribute quotes to a specific person and/or a specific port site. Instead, we focused on broader descriptions of a greater number of initiatives, with a focus on what the site personnel identified as positive and promising. Also, we note limitations or problems in the programs and technology we observed where possible, but we were generally not in a position to identify specific gaps in security that we observed. In most cases, these weaknesses were due to the "newness" of the initiative, technology or areas that port management were already addressing through additional training. In general, the port sites were very generous in providing us access to the full range of port activities and security initiatives. Nevertheless, research on sensitive topics involves some compromises. Along with great access to sensitive data comes the responsibility to safeguard it, where necessary.

Research Tasks

The research team proposed, and implemented, a sequenced series of tasks in order to meet the project's goal of identifying and describing "promising practices" being used by local public and private agencies to defend America's ports from terrorist attacks. This section summarizes those tasks.

Task 1: Generate Background Information about Ports and Port Security

The research team read and abstracted available material concerning America's ports, their structure, and their security concerns. The team was particularly fortunate to be able to enlist the assistance and support of the American Association of Port Authorities (AAPA), the professional association representing the nation's port authorities. In particular, Dr. Rex Sherman, the Director of Research of AAPA, provided complete access to his library and professional contacts. In addition, the research team conducted extensive literature reviews of academic and government publications concerning ports and port security.

To further prepare themselves, members of the research team conducted extensive interviews with experts in the field of port security and attended several port security seminars.

Finally, team members conducted familiarity visits to the ports of San Diego, Baltimore, Los Angeles, Long Beach, Corpus Christi, and Miami in order to obtain firsthand familiarity with the operations of ports and the concerns of their stakeholders.

Task 2: Create Project Advisory Board

The team then constituted a project advisory board of representatives of the stakeholders in America's ports. In particular, the board consisted of representatives of the following organizations:

- American Association of Port Authorities
- United States Coast Guard
- United States Department of Homeland Security
- United States Maritime Administration
- International Association of Airport/Seaport Police
- National Cargo Security Council
- Chamber of Shipping of America
- International Council of Cruise Lines
- National Association of Warehouse Employers
- American Trucking Association
- American Association of Railroads

The board met early in the project and provided advice about the goal of the project and how best to achieve it. The members provided valuable insights into their perspectives on the issue of port security, made recommendations concerning literature to be reviewed, and provided advice about issues to be addressed and methods to be used. The board members also reviewed a draft site visit protocol and made recommendations about ports that should be visited.

Task 3: Create a Site Visit Protocol

The research team created a site visit protocol to be used in conducting site visits to several ports. A draft of the protocol was reviewed and approved by the advisory board, representatives of the Department of Justice, and the project's Institutional Review Board. A copy of the protocol is included as Appendix A of this report.

Task 4: Conduct Site Visits to Ports

With the assistance of the project advisory board, the research team selected 17 ports to be visited. As indicated in the protocol, the following criteria were used in selecting the sites visited:

- They should represent ports with wide variation in the tonnage of cargo, the volume of containers, and the number of cruise vessels handled annually;
- They should represent a mixture of ports that handle cargo ships, passenger liners, and naval vessels;
- They should represent a mixture of landlord ports, operating ports, and limited operating ports;

- They should represent a variety of law enforcement structures: port authority police agencies, port authority security departments, reliance on local law enforcement, and contracted law enforcement;
- They should reflect all major deep water locations (the Atlantic Ocean, the Pacific Ocean, and the Gulf of Mexico); and
- They should be willing to cooperate with the provisions of the study.
- For budgetary reasons, we also considered the location of the port. Some sites were selected in geographic clusters, allowing, where possible, more than one port per trip.

Distinguishing Features of Ports in this Study

Using these criteria, the research team made site visits to 17 ports: San Diego, CA; Los Angeles, CA; Long Beach, CA; Jacksonville, FL; Tampa, FL; Ft. Lauderdale, FL; Miami, FL; New Orleans, LA; Houston, TX; Galveston, TX; Texas City, TX; Charleston, SC; Savannah, GA; Port of Virginia, VA; Boston, MA; Seattle, WA; and Tacoma, WA.

As the protocol indicates, members of the site visit team interviewed a wide range of persons involved in managing the port and providing for its security. In all sites, persons interviewed were to include, but not necessarily be limited to, the following, or their representatives:

- Captain of the Port and other U.S. Coast Guard representatives;
- Port Authority Manager/Director;
- Port Security Director;
- Facility Security Officers;
- Port Authority Police Chief (if any) and officers;
- Representatives of local municipal, county, and state police agencies involved with port security;
- Representatives of other federal government agencies involved with port security, including the FBI, U.S. Navy, DEA, and ICE;
- Representatives from private security agencies, if appropriate;
- Representatives of local fire departments;
- Representatives of tenants in the port, if appropriate;
- Representatives of unions and stevedores; and
- Others, as identified.

At each site, the evaluation team addressed the following issues:

- What is the management structure of the port? Does it operate as a landlord port, an operating port, or a limited operating port?
- Is there a Port Authority police department?
- Is there a Port Authority security department?
- What are the primary security concerns in and around the port?
- Has the port security plan(s) been completed? Who produced it? To what extent has the plan been reviewed, approved, and implemented?
- What agency/agencies are responsible for providing security at the port? How are their efforts coordinated?
- What is the nature of the relationship among the principal stakeholders involved in providing security—port authority police, municipal police, county law enforcement

agencies, other government agencies, and private security?

- Do local law enforcement and/or private security participate in the maritime security committee? Do other law enforcement agencies? Private security?
- What sources of intelligence do local law enforcement and/or private security have with regard to security threats? Is it shared with other agencies? Which other agencies?
- Who is represented on the Maritime Regional Security Committee (or its equivalent)? How often does it meet? What role does it play?
- Do local law enforcement agencies and/or private security work with the local Joint Terrorism Task Force?
- Do law enforcement agencies and/or private security assist in conducting background checks conducted for personnel working at the port? For what type of workers? By whom? What are the criteria for employment?
- Do law enforcement agencies and/or private security patrol the perimeters of the port—landside and seaside?
- Do law enforcement agencies and/or private security enforce access control for entry to the port?
- Do law enforcement and/or private security require credentials for persons entering the port? What type of information is contained on these credentials? Are different types of credentials required for different types of people entering the port?
- Do law enforcement and/or private security inspect containers and other cargo coming into and leaving the port? Do law enforcement and/or private security secure the public spaces within the port?
- Are law enforcement and/or private security responsible for access control to separate terminals within the port?
- Do law enforcement and/or private security limit access to certain parts of the port to people with special credentials?
- What training regarding port security has been provided to law enforcement and private security? How many hours? By whom? To whom? What was the nature of the training? Do you feel it is sufficient?
- What plans exist concerning how to respond to a terrorist attack if it actually occurred? Have you conducted exercises to practice implementing those plans? How many? With whom?
- What plans have been made to mediate the effects of a possible attack? What roles are to be played by which agencies?
- What plans have been made to restore the port to operational condition?

A brief description of each of these ports is provided below.

Port of San Diego

The San Diego Unified Port District is a special government entity formed in 1962 by an act of the California legislature in order to manage San Diego Harbor and administer the public lands along San Diego Bay.[21] Its jurisdiction includes land in five member cities of the Port

[21] The port district came about as a result of a statewide Progressive revolt which broke the stranglehold of railroads over Sacramento politics in 1910. In the 1911 legislative session, a coalition of Oakland, San Diego, and Los Angeles won a fight that allowed them to create powerful port authorities, allowing them to "municipalize" their

District, including San Diego, Chula Vista, Coronado, Imperial Beach, and National City. In addition to port facilities, the district leases and manages land along the port, including 16 bay-front parks and commercial property occupied by more than 350 tenant businesses. The district is governed by a board of port commissioners appointed by the city councils of the five cities represented by the district. Three of the commissioners are from San Diego; one is from National City; one is from Chula Vista; one is from Coronado; and one is from Imperial Beach.

San Diego harbor is the site of a large number of military installations, including the Naval Air Station, North Island; the Naval Amphibious Base, Coronado; Naval Station, San Diego; Naval Base Point Loma; the U.S. Marine Corps Recruit Depot; the U.S. Marine Corps Air Station, Miramar; the U.S. Marine Corps Base, Camp Pendleton; the Space and Naval Warfare Systems Command; and the Fort Rosecrans Military Reservation. The port is also designated as a "strategic port," assigned to make port facilities and services available during a defense mobilization. It is one of 12 ports designated a "controlled port," with controls on access for vessels from certain countries, due to national security issues. Critical facilities, in addition to cruise ships and naval vessels, include the Coronado Bridge, a nuclear fuel storage facility, and a power plant near the water's edge.

The port ranks 24th in container traffic, 11th in passengers, and 99th in total tonnage. Primary inbound cargoes include vehicles, lumber, cement, newsprint, sand, cut paper, fertilizer, and fresh fruit and vegetables. Primary outbound cargoes are soda ash, potash, and sodium sulfate. It is an operating port, managed by a board of commissioners appointed by the city council for four-year terms. It has its own San Diego Harbor Police Department, responsible for policing San Diego Bay, the San Diego International Airport, and all Tidelands around the bay, throughout all five member cities of the Port District. Private security is involved only at the cruise terminal, when ships are in harbor. A Joint Operations Center, involving the San Diego Harbor Police, San Diego Police, U.S. Coast Guard, U.S. Navy, and other agencies has been established. Grant funds have supported the development of a system capable of analyzing integrated databases, using data from several agencies in the Southern California area.

Port of Los Angeles

The Port of Los Angeles is a department of the City of Los Angeles, the Los Angeles Harbor Department. The port is operated and managed under a State Tidelands Trust that grants local municipalities jurisdiction over ports and stipulates that activities must be related to commerce, navigation, and fisheries. San Pedro Bay was an active shipping center in 1897 when a federal panel selected it over other coastal communities as the site for development of a major port. In 1906, the City of Los Angeles annexed a 16-mile strip of unincorporated land from its southern border to a waterfront tract in the bay, which was christened Harbor City. At the end of 1907, on the eve of the consolidation of San Pedro and Wilmington with Los Angeles, the Los Angeles City Council created the Los Angeles Board of Harbor Commissioners, giving it control over the Los Angeles Harbor Department, a city agency responsible for managing and supervising the harbor district. The board members, appointed by the mayor and confirmed by the city council, serve for a term of five years. As a proprietary and self-sustaining department, the port is not supported by taxes. Instead, revenue is derived from fees for shipping services such as dockage, wharfage, pilotage, storage, property rentals, royalties, and other port services.

---

waterfronts by reclaiming state-owned tidelands for port development. On the other hand, San Francisco, which had abdicated administration of its waterfront to a state commission during the so-called "bulkhead wars" of the 1850s, failed to wrest port improvements from the state. (Davis, Mayhew, and Miller, 2003, p. 38).

The Harbor Department owns the majority of wharves and piers in the harbor area, and disburses leases for industrial sites and oil drilling.

The port ranks first in container traffic, fifth in passenger traffic, and 14th in total tonnage. Primary inbound cargoes include containerized furniture, apparel, computer equipment, toys, and electronic products. Primary outbound cargoes include containerized wastepaper, resins and plastics, pet and animal feeds, cotton, and mixed scrap metal. The port's petroleum facility handles one-half of the state's needs.

Considered a landlord port, the Port of Los Angeles leases its property to tenants who then, in turn, operate their own facilities. The Port of Los Angeles abuts the Port of Long Beach which, although an economic competitor, is a partner in many endeavors, including port security. The Port of Los Angeles has its own police department, although it works closely with the Los Angeles Police Department. Also, private security guards, who are employed by the individual terminal operators, are found at the port.

Port of Long Beach

In 1909, voters in Long Beach approved a municipal bond issue for harbor improvement. In 1911, the state legislature approved a Tidelands grant to Long Beach, giving the city the right to manage and develop the Harbor District for commerce, navigation, fisheries, and recreation. In June of that year, a municipally owned pier was completed and the first ship docked there. In 1931, the Long Beach City Charter established the boundaries of the Harbor District, and created the Harbor Commission to set policy, as well as the Long Beach Harbor Department to carry out those policies. In 1936, oil was discovered in the area. For the next three decades, oil pumps provided the city with a greater source of revenue than shipping. The pumping also caused subsidence of the land and lateral shifting over a widespread area, resulting in costly engineering problems. The port is a department of the City of Long Beach. The Long Beach Board of Harbor Commissioners, whose five members are appointed by the mayor and confirmed by the city council, governs the Harbor District, which includes the port. In accordance with the state Tidelands Trust, port operations are not financed with tax revenues; instead, port funds are earned from commerce that moves through the port.

The Port of Long Beach is one of 13 commercial ports designated as a "strategic port," with orders from MARAD and the DOD defining how it should make port facilities and services available to meet anticipated defense agency requirements during a mobilization. It ranks second in container traffic, seventh in passenger traffic, and fifth in total tonnage. Primary inbound traffic includes petrochemicals, barite, rutile, and forest products. Primary outbound products include petrochemical products, rice, bagged goods, and vegetable oil. Long Beach is a "landlord port," which means that the Board of Harbor Commissioners leases port facilities to private companies (shipping lines and cargo-handling firms) who then contract with union longshore workers to operate the shipping terminals. It does not have its own police department, but instead has a Harbor Patrol, which is uniformed but unarmed. It relies on the Long Beach Police Department, which has its own harbor unit, for law enforcement. Private security is hired by individual tenants.

Port of Jacksonville

The Jacksonville Port Authority (JAXPORT) is an independent government agency created by the Florida legislature in 1963. It is governed by a seven-member board, with three members appointed by Florida's governor and four appointed by Jacksonville's mayor. Each

board member serves a four-year term. The port consists of three public marine terminals (the Blount Island Marine Terminal, the Talleyrand Marine Terminal, and the Dames Point Marine Terminal) and the temporary JAXPORT Cruise Terminal. The port receives no public dollars; operating expenses are funded by means of user fees, leases, and other charges paid by tenants.

The port is a "strategic port," with obligations to support defense mobilizations. Naval Air Station Jacksonville is a military airport located four miles from the center of Jacksonville, and is the third-largest naval installation in the United States. JAXPORT ranks 13th in container traffic, 13th in passenger traffic, and 38th in total tonnage. Primary inbound traffic includes coal and coke, crude and fuel oil, gypsum, limestone, automobiles, granite, paper and paperboard waste, cement, stones and pebbles, steel wire rods, crude minerals, and wood pulp. Primary outbound traffic includes grocery products, fresh and frozen goods, automobiles, beer and ale, dextrose and glucose, vegetables, meat, non-alcoholic beverages, wood pulp, milk and dairy products, and trucks.

As a landlord port, JAXPORT rents its facilities to private tenants. JAXPORT contracts with the Jacksonville Sheriff's Office for law enforcement. It has its own security department that provides access control and non-law enforcement security services. Security officers are responsible to sheriff's deputies. Also, individual tenants hire their own private security.

Port of Tampa

The Hillsborough County Port district was established by the Florida legislature in its current form in 1995. The governing body is the Tampa Port Authority, comprised of five members, three of whom are appointed by the Governor, one of whom is a member, ex officio, of the Board of County Commissioners of Hillsborough County, and one of whom is the mayor of the City of Tampa, ex officio.

The port is ranked 16th nationally in total tonnage but is not among leading ports in container traffic, since most cargo is bulk or semi-bulk. The port is ranked eighth nationally in passenger traffic. The port's primary inbound cargoes are petroleum, and primary outbound cargoes are phosphates.

As a limited operating port, Tampa is characterized by a complicated quilt-like mixture of privately-operated and port-operated facilities. The Tampa Port Authority (TPA) contracts with the Hillsborough County Sheriff's Office (HCSO) for law enforcement services. TPA also has its own security division, whose employees are responsible for entry control; these security officers operate independently of the HCSO.

Port Everglades

Despite its name, this port is not a part of the wetland ecosystem known as the Florida Everglades. It is, instead, located on the southeastern coast of the Florida peninsula within the three cities of Fort Lauderdale, Hollywood, and Dania Beach, as well as unincorporated Broward County. Port Everglades, originally known as Lake Mabel or Bay Mabel Harbor, was officially established as a deep-water harbor in 1927 by the Florida state legislature. The port is a department of the Broward county government. It functions as an "Enterprise Fund" that competes with other public- and private-sector organizations for customers and cargoes. As an Enterprise Fund, it generates its own revenue to pay for expenses and capital improvements.

With annual operating revenues exceeding $105 million in 2005, Port Everglades experienced 5,901 total ship calls, generated container cargo revenue of more than $24 million and cruise revenue of $30 million, and handled 5 million tons of container cargo and 3.8 million

cruise passengers. Nearly 20 cruise lines and 35 cargo shipping lines conduct business at Port Everglades. Port Everglades is known as one of the finest cruise ports. It ranks second in the nation in terms of the number of passengers handled, and is able to handle 14 cruise ships at one time. It also ranks 14th in terms of container traffic and 32nd in total tonnage. In addition, the port handles a sizeable amount of petroleum products. Primary inbound cargoes include gasoline, aviation fuel and other petroleum products, cement, apparel, fruits, vegetables, ceramic and mosaic tiles, as well as beer and ale. Primary outbound cargoes include grocery products, fabrics, building and construction material, paper, poultry, automobile parts, logs and lumber, automobiles, gasoline and aviation fuel, trucks, non-alcoholic beverages, and fruits.

A limited operating port, Port Lauderdale leases some of its facilities for tenants and conducts its own operations in other parts of the port. The Broward County Sheriff's Office (BCSO) has a contract to provide law enforcement services on the port premises. In addition, the BCSO has recently contracted to provide broader security services, including access control, taking the place of a private security firm. Tenants contract with their own private security firms to provide security within their designated areas.

Port of Miami

Officially called the Dante B. Fascell Port of Miami-Dade, the port is a department of the Miami-Dade County government. The port ranks first in the nation in passenger traffic, 12th in the nation in container traffic, and 66th in total tonnage. The port can handle up to six passenger ships at once, each with 3,000 to 5,000 passengers. Primary inbound cargoes are stone, clay and cement tiles; fruits and vegetables; apparel; alcoholic beverages; lumber and wood; iron, steel and other metal products; fabricated wood products; non-alcoholic beverages; and paper. Primary outbound cargoes are paper; textiles; food products; building materials; spare parts; trucks and buses; iron, steel and other metals; and machinery and industrial equipment.

Miami operates as a landlord port, renting its facilities to various tenants. The Miami-Dade Police Department is responsible for law enforcement at the port, and maintains a sub-station at the port. The port also has a non-sworn complement of civilian Seaport Safety and Security personnel. At the Port of Miami, tenants hire their own private security guards.

Port of New Orleans

The Port of New Orleans, stretched over 26 miles of the Mississippi River, is governed by a Board of Commissioners, made up of seven unpaid commissioners who serve five-year staggered terms. The Governor of Louisiana appoints board members from a list of three nominees submitted by 19 local business, civic, labor, education, and maritime groups. The board is required to reflect the three-parish (county) jurisdiction of the port. Four members are selected from Orleans Parish, two from Jefferson Parish, and one from St. Bernard Parish.

The Port of New Orleans ranks 17th in container traffic, 9th in passenger traffic, and 7th in total tonnage. Primary inbound cargoes are steel, rubber, plywood, and coffee. Primary outbound cargoes include forest products, steel, foodstuff and chemicals.

As a landlord port, the Port of New Orleans rents its facilities to private tenants. The port has its own Harbor Police Department, which is responsible for law enforcement in the port. Access control is the responsibility of private security hired by the port. Tenants hire their own private security firms to maintain security in their leased spaces.

Port of Galveston

First designated a port and customs entry point by the Congress of Mexico in 1825, the port began as a private company known as the Galveston Wharf and Cotton Press company. After years of dispute, the city gradually took control of the facilities between 1940 and 1947, creating the Port of Galveston (commonly known as "the Galveston Wharves") as a department of the City of Galveston.

Although the Port of Galveston ranks only 27th in the nation in container traffic, and 61st in total tonnage, the Port of Galveston ranks sixth in the nation in passenger traffic. The latter is a dramatic development, since its container terminal was opened only five years ago. Primary inbound cargoes include bulk fertilizer; bulk cement; bulk liquids; bananas; and other fresh fruit; and roll on/roll off cargoes. Primary outbound cargoes include primarily bulk grain.

As a landlord port, Galveston leases its facilities to private tenants. It has its own port police department, responsible for perimeter and access control as well as patrolling the premises of the port. Some tenants hire their own private security guards.

Port of Texas City

The Port of Texas City is located on the western shore of Galveston Bay, Texas, approximately 35 miles south of Houston, and 18 miles north of Galveston. A privately owned port, the Port of Texas City/Texas City Terminal Railway Company, has as its shareholders the Union Pacific and Burlington Northern Santa Fe railroads, whose connections provide important links to the port. The port handles no container or passenger traffic, but ranks 9th in total tonnage. Most of its cargo consists of a variety of chemicals and petrochemical products. The facilities on or near the Port of Texas City produce a concentrated cauldron of chemicals, including, as they are called in the petrochemical trade, volatile organic compounds (VOCs), or as they are called in the shipping industry, Certain Dangerous Cargos (CDCs). Individually, and particularly in combination, these chemicals can be explosive, toxic, noxious, and deadly.

As a landlord port, Texas City does not operate any docks, take title to any product, or tie up any ships or barges. It survives by leasing property on the port to twelve tenants. In the event of a crime, such as an assault involving employees, a security guard will call 911 to contact the Texas City Police Department. In normal circumstances, the police do not patrol the internal area of the port. The police department does not have patrol boats. However, the Galveston Sheriff's Department periodically patrols the port in one of its patrol boats to provide visibility and to detect suspicious activity, as part of its Homeland Security route. The port also contracts with a private security company to provide access control and patrol the common area of the port. Tenants hire their own security guards to protect their leased areas. The Texas City Police Department would be called upon only in cases that could not be handled by private security.

Port of Houston

The Port of Houston Authority is an autonomous political subdivision of the State of Texas, authorized by a 1927 Act of the Texas legislature. The Authority is governed by a seven-member commission. The City of Houston and the Harris County Commissioners Court each appoint two commissioners; these two government entities also jointly appoint the chairman of the Port Commission. The Harris County Mayors' and Councils' Association and the City of Pasadena each appoint one commissioner. The Port of Houston is considered a combination of the Port of Houston Authority and the 150-plus private industrial companies along the Houston

Ship Channel, stretching 26 miles to Galveston Bay. The Authority consists of several individual terminals, including Barbours Cut Container Terminal, the Turning Basin Terminal, the Woodhouse Terminal, the Jacintoport Terminal, the Care Terminal, as well as other facilities such as the Bayport Industrial Complex, the Bulk Materials Handling Plant, Wharf 32, and Houston Public Elevator Number 2.

The Port of Houston ranks 10th in container traffic, 15th in passenger traffic, and 2nd in total tonnage. The port handles 62 percent of the nation's chemical traffic and 38 percent of its gasoline traffic. Primary inbound cargoes include petroleum and petroleum products, crude fertilizers and minerals, iron and steel, organic chemicals, and inorganic chemicals. Primary export cargoes include petroleum and petroleum products, cereals and cereal products, organic chemicals, plastics, and inorganic chemicals.

As a limited operating port, Houston leases some of its facilities and conducts its own operations from others. The port has its own police department, but access control is handled by a private security firm contractor. Tenants hire their own private security.

Port of Charleston

The Port of Charleston is one of three port facilities (along with the Port of Georgetown and the Port of Port Royal) owned and operated under the auspices of the South Carolina State Ports Authority (SCSPA). The SCSPA, an instrumentality of the State of South Carolina, has a governing authority of nine members, appointed by the Governor, with the advice and consent of the Senate, for terms of seven years each. It is designated as a "strategic port," with orders from the United States Maritime Administration (an agency of the United States Department of Transportation that maintains the National Defense Reserve Fleet) and the Department of Defense (DOD) defining how it should make port facilities and services available to meet anticipated defense agency requirements during a mobilization.

The Port of Charleston ranks fifth nationally in container traffic, 19th in passenger traffic, and 34th in total tonnage. The port has five major terminals: Columbus Street Terminal, North Charleston Terminal, Wando Welch Terminal, Union Pier Terminal, and Veterans Terminal, spread throughout the Charleston area. Primary inbound cargoes include consumer goods, iron and steel, chemicals, foodstuffs, textiles, and machinery. Primary outbound cargoes include chemicals, paper products, wood pulp, foodstuffs, machinery, vehicles, and clay.

Charleston is an operating port. As a result, the SCSPA owns the terminals and operates them with its own staff. SCSPA works all container cranes at the port, runs the container yard equipment, and operates gates on all terminals. The only exceptions are the licensed operators at the port, who lease terminal space and operate their own yards and gates. SCSPA staff members also operate the dockside container cranes and the yard equipment for licensed operators. Law enforcement is provided by the South Carolina Ports Authority Police Department. Terminal leasees can hire their own private security guards. The Port of Charleston is also the location for Operation Seahawk, a partnership of 47 federal, state, and local agencies under the leadership of the U.S. Attorney, which has received significant funding to conduct joint anti-terrorism efforts.

Port of Savannah

The Port of Savannah is one of four ports owned and operated by the Georgia Ports Authority (GPA), a quasi-state agency, governed by a 13-member Board of Directors. Board members are appointed by the Governor, from the state at large, to serve four-year, staggered terms. The port is a "strategic port," with obligations to support defense mobilizations. The Port

of Savannah is home to one of the largest single-terminal container facilities of its kind on the U.S. East and Gulf coasts, and is one of the fastest-growing ports in the nation. The Port of Savannah was the nation's eleventh busiest waterborne freight gateway for international trade by value of shipments in 2003. In a 10-year period, the Port of Savannah has nearly tripled its exports, and will soon significantly increase its dock capacity with the construction of a new container berth. The Port of Savannah is a major point for imports from South and Central America and the Caribbean and for exports to Asian countries. By tonnage, Venezuela is its largest origin country for imports, while Japan is the port's largest destination country for exports. Savannah ranks 9th in container traffic and 28th in total tonnage. It has no passenger traffic. It has two cargo terminals, Garden City Terminal, a container facility, and Ocean Terminal, a break-bulk facility. Primary inbound cargoes are petroleum products, crude petroleum, coal, sugar, and furniture. The leading outbound cargoes are clays, wood pulp, paper and paper board, meat, and wood.

Savannah is an operating port, owning and operating its own terminals. Law enforcement is provided by the South Carolina Ports Authority Police Department. The GPA has increased its force to nearly 80 police officers (a greater than 100-percent increase compared to immediately before 9/11) and improved its training program. The switch to a predominately certified GPA police force occurred in 1988. These extra security costs have been addressed only recently through security surcharges. In addition to field, warehouse and dock patrols, gates are fully staffed by Port Police to verify that all containers, RoRo cargo, breakbulk cargo, vans and private vehicles transiting the terminals are authorized for entry and departure. Port Police Officers are certified through the Georgia Peace Officers Standards & Training (POST) Council as Certified Law Enforcement Professionals and are empowered with the same authority and arrest powers as any other police officer in the State of Georgia. The GPA Port Police Department maintains a close working relationship with all federal, state and local law enforcement agencies. There are only a couple of tenants on GPA property, and they have their own security force that coordinates its efforts with the GPA Police. In coordination with the Coast Guard, the Savannah Chatham Police Department has a marine division that patrols the waters around the port. The Port of Savannah holds annual exercises and drills. These one-day multi-layered training exercises are designed to refine, rehearse and validate homeland security plans for providing military support for civil authorities. These exercises bring together members of the Georgia National Guard's 4th Civil Support Team, U.S. Customs and Border Protection, the Georgia State Patrol, the Chatham Emergency Management Agency, the Chatham County Emergency Management Agency, the Georgia Bureau of Investigation, the Coast Guard, Chatham County Explosive Ordnance Disposal, GPA Police, and a number of other federal, state and local first responders. This exercise helps the various responding agencies to identify areas of responsibility and coordination.

Port of Virginia

The Port of Virginia is operated by the Virginia Port Authority (VPA), an agency of the Commonwealth of Virginia, reporting to the Secretary of Transportation. The 11 members of the board are appointed by the Governor for staggered five-year terms. The port facilities are operated by the VPA's private operating company, Virginia International Terminals, Inc. The port receives no money from the state's general fund; rather, earnings from these facilities cover the operational costs of the port. The VPA owns Norfolk International Terminal, Newport News

Marine Terminal, and Portsmouth Marine Terminal, all in the Hampton Roads area.[22] Hampton Roads is the world's largest U.S. Navy base, consisting of several installations, including Naval Station Norfolk, Norfolk Naval Shipyard, Naval Amphibious Base Little Creek, Naval Air Station Oceana, and Naval Weapons Station Yorktown. Hampton Roads is also the homeport of the Atlantic Fleet and the location of Northrop Grumman Newport News, a privately owned company that builds the *Nimitz*-class aircraft carrier. The ports in the Hampton Roads area (including Norfolk, Newport News, Jamestown, Yorktown, and Portsmouth) have been designated a "controlled port," meaning they have access controls for vessels from certain countries for national security reasons.

The Port of Virginia ranks sixth in terms of container traffic and 15th in terms of total tonnage. It has no passenger traffic. Primary inbound cargoes include tobacco, auto engines and parts, natural rubber, paper and paperboard, construction and building equipment, alcoholic beverages, metal manufactures, cocoa beans, machinery parts, and manufactured or processed food. Outbound cargoes include logs and lumber, paper and paper board, wood pulp, tobacco, auto parts, alcoholic beverages, poultry, pet and animal feeds, staple fibers and fabrics, and alcohol and alcohol derivatives.

As an operating port, the port authority operates all facilities on the general area of the port, although tenants have their own employees in their leased terminals. Law enforcement services are provided by the Virginia Port Authority Police Department. No private security is allowed on the premises. Also, a Joint Harbor Operations Center (JHOC) has been established, involving the U.S. Navy and the Coast Guard.

Port of Boston

The Port of Boston operates under the auspices of the Massachusetts Port Authority (known as Massport), established by the Massachusetts legislature in 1959 as an independent public authority. It is not part of the state government, although its board is appointed by the governor for staggered seven-year terms. Massport receives no state taxpayer funds for its operations. Instead, it is a revenue bond authority, and all of its funds are generated by these bonds and through user fees charged at the facilities it operates. Massport also owns Logan Airport and approximately 500 acres of property in the Boston area. The port owns Conley Terminal, for containerized cargo, and Moran Terminal, currently leased to Boston Autoport for the import and distribution of automobiles. In addition, the port owns the Black Falcon Cruise Terminal (called Cruiseport Boston).

The Port of Boston ranks 21st in container traffic, 18th in passenger traffic, and 31st in total tonnage. Primary inbound cargoes include automobiles, beer and wine, games and sport equipment, ceramic tiles, fish and shellfish, footwear, furniture, and paper. Primary outbound cargoes include fish and fish products, hides and skins, household goods, logs and lumber, metal waste and scrap, and paper and waste paper resin.

As an operating port, the port authority operates all general facilities except for Autoport and cruise operations. Law enforcement is provided by the Massport Police Department, part of the Massport, backed by Troop F of the Massachusetts State Police, stationed at Logan Airport. The Boston Police Department also has a Harbor Marine Unit which services the harbor area. Of major security concern are the frequent deliveries of Liquified Natural Gas (LNG) tankers which

[22] The VPA also owns the Virginia Inland Port, in Front Royal. The Port of Richmond is a separate port, not under the auspices of the VPA.

traverse the port facilities to the LNG terminal in Everett. Multiple federal, state, municipal and port law enforcement agencies work together to escort and protect these ships.

Port of Seattle

The Port of Seattle is a municipal corporation created in 1911 by the voters of King County. Five commissioners are elected at large by the voters of King County to serve four-year terms. The corporation, under the auspices of its Aviation Division, operates Seattle-Tacoma International Airport (Sea-Tac). In addition to the airport, the port owns the Shilsle Bay Marina; the Maritime Industrial Center and Fishermen's Terminal on Salmon Bay; cargo terminals and a grain elevator on Smith Cove; and numerous cargo terminals on Elliot Bay, Harbor Island, and the Duwamish Waterway. The Port of Seattle also controls recreational and commercial moorage facilities and two cruise ship terminals.

The Port of Seattle is one of the largest container and breakbulk cargo centers on the west coast of the United States. Closer to Asia than any other major U.S. port other than the Port of Tacoma, Seattle is a premier gateway for products moving to and from North America. The Port of Seattle's rail and road access make it an attractive choice for fast cargo transshipment, supporting a volume of 2.1 million Ton Equivalent Units, or TEUs (20-foot equivalent unit containers) through the seaport. The Seattle seaport was North America's fastest-growing container port in 2005, the second year in a row it has grown faster on a percentage basis than any other U.S. port. The port ranks 8th in container traffic, 10th in passenger traffic, and 37th in total tonnage. Primary inbound cargoes include apparel, games, video games, footwear, motor vehicle parts, office and data processing machines, audio equipment, electrical/electronic equipment and parts, toys, furniture, and telecom, sound and recording equipment. Primary outbound cargoes include inorganic chemicals; beef, pork, and poultry; oilseeds; industrial equipment; frozen fish; animal feeds; motor vehicle parts; engines; paper; and frozen vegetables. There is a heavy Navy presence in the Puget Sound area, including Naval Station Everett, naval Base Kitsap, and Naval Air Station Whidbey Island. A major concern is the Washington State Ferries system, which operates the largest ferry fleet in the united State. Twenty-eight ferries cross Puget Sound and its inland waterways, carrying more than 26 million passengers to 20 different ports of call.

As a limited operating port, the Port of Seattle leases some of its facilities to private tenants but operates certain facilities on its own. The port has its own police department, and provides the primary law enforcement response within the geographical boundaries of the Port of Seattle, including Seattle-Tacoma International Airport and a portion of the surrounding residential and commercial properties. Port Police also patrol major portions of the Seattle waterfront and Elliott Bay. The Port of Seattle has a mix of port-owned and port-operated property and tenants. Created in 1972, the Port of Seattle Police Department includes 108 commissioned officers and 31 support staff members. The Department has its own 911 call center that dispatches for the Port Police and Fire Departments as well as the Burlington Northern Santa Fe Police Department. The Port of Seattle Police is a certified law enforcement agency with sworn officers. The Port of Seattle Police has a diverse set of special teams that can handle a range of terrorist threats, including a dive team, boat team, bomb disposal unit, crisis negotiation team, criminal investigations unit, K-9 unit, and a special response/tactical team. These capabilities are not typically found in a port police agency. The port police have these extensive capabilities in part due to their responsibilities for not only the seaport, but also the Seattle-Tacoma International Airport and a portion of the surrounding residential and

commercial properties. The port also has a security department responsible for overall security of the port. Some of the tenants also hire their own private security guards. The Washington State Police are responsible for law enforcement and security on the ferry system.

Port of Tacoma

The Port of Tacoma is an independent municipal organization that operates under state-enabling legislation that permits ports to be organized as special purpose districts. The port was established by the voters of Pierce County in 1918. A five-member Port of Tacoma Commission is the governing body of the port. Commissioners are elected to four-year terms.

From a distribution perspective, more than 70 percent of the Port's international container cargo comes from, or is going to, the central and eastern regions of North America--making Tacoma a true "Gateway Port." The Port also handles more than 70 percent of the marine cargo moving between the lower 48 states and Alaska. As a leading North American seaport, the Port of Tacoma's terminals handle more than $29 billion in annual trade and 1.8 million TEUs, and are considered a major center for bulk, breakbulk, and project/heavy lift cargoes as well as automobiles. Since 1982, when the first Port of Tacoma economic impact study was conducted, the Port's jobs impact has increased nearly 400 percent, and now more than 1,350 Washington state firms import and/or export goods directly through the Port of Tacoma. The Port of Tacoma is comprised of eight modern terminals, each having its own specific berth, ramp and equipment configurations: TOTE Terminal; Husky Terminal; Washington United Terminals (WUT); Pierce County Terminal; Olympic Container Terminal; Terminal 7-A/B; APM Terminals; and Cargill Grain Terminal. The Port of Tacoma has one of the most extensive rail systems that is capable of providing direct access to the docks in the United States. The rail yards, within the Port of Tacoma facilities, are the jurisdiction of a police force separate from the Port Security. As armed peace officers, these railroad special agents are mandated to protect and safeguard railroad assets including personnel, property, information, and customer lading.

The Port of Tacoma not only plays a significant role in the basic commerce of the local region and the larger continental United States, but it also serves as a strategic military transport site for U.S. military operations and has been used to stage a variety of military and Homeland Security exercises over the years, such as Puget Thunder in 2000, Seahawk in 2002, Maritime Terrorism Response (MTR) in 2005, and Evergreen Sentry in 2006. The strategic nature of the Port of Tacoma cannot be overstated, considering the fact that the nearby Fort Lewis and McChord military bases are used for military mobilization processing functions and were designated as Joint Pre-Deployment/ Mobilization Sites for the military in 2005, a function which the Port of Tacoma has supported for many years prior to this designation.

The port ranks 7th in container traffic and 30th in total tonnage. It has no passenger traffic. Primary inbound cargoes include vehicles and auto parts, machinery, electrical equipment and components, footwear, toys, and sports equipment. Primary outbound cargoes include grain, machinery, meat and poultry, vehicles and auto parts, and inorganic chemicals. As a limited operating port, the port leases many of its facilities to private tenants but operates some of them itself.

The port has an armed, non-sworn patrol force, and relies on the Tacoma Police Department for law enforcement. The primary port security provider, the Port Security team, consists of approximately 25 officers, including one Chief and one Director. Additionally, all Port Security officers receive official police training from the police academy, which includes training in firearms, use of force, less than lethal tactics, and use of handcuffs. Port Security

personnel have also received special training in intelligence analysis, and Port Security is a member of the larger national Joint Terrorism Task Force (JTTF) partnership and team. In support of the intelligence function, the Port Security force produces a number of intelligence reports for distribution to key stakeholders. In addition to Port-owned and -operated properties, a large portion of Port property is occupied by a variety of private landowners or operators. Whether the tenants own or lease property, they each provide their own access and control measures, and Port Security personnel cannot access these areas without permission of the individual tenants. Each tenant, however, is required to draft and supply a security plan to the U.S. Coast Guard that includes details on access to the terminal and the security training they provide to employees. But there are no formal arrangements for these tenant-based security plans to be shared with Port Security personnel. In instances where a tenant or a port employee notices suspicious activities, Port Security will be called upon to respond. However, in any instance where a crime has been committed, tenants and port personnel call the Tacoma Police Department for official police assistance.

IV. Research Findings: Promising Practices

As described in the methods section, at each of the 17 ports we visited, we sought to identify practices, programs, and policies that appeared worthy of further examination and testing. This section describes these promising practices used by law enforcement and private security to prevent America's deep-draft ports from being attacked by terrorists. The modesty of the appellation "promising" must be stressed. These practices have not been evaluated in even the broadest sense of the term. None of them has been randomly assigned to experimental and control groups, or analyzed in relation to a comparison group. Even comparisons to pre-implementation performance produce no empirical results, since, fortunately, no terrorist incidents have occurred at any of the ports visited.

Nevertheless, our site visits and discussions with port security professionals have highlighted certain practices, programs, and policies that stand out from others, because of their innovativeness, comprehensiveness, or rigorous implementation. This section of the report summarizes the most notable of these "promising" practices being used by local law enforcement, ports, or private security agencies at the ports visited during this study. Unless there are unique regional variations, this discussion explicitly excludes from its focus programs being implemented by federal agencies, such as the Department of Homeland Security (Coast Guard, Customs and Border Protection, Immigration and Customs Enforcement); or the Department of Justice (Federal Bureau of Investigation; Bureau of Alcohol, Tobacco, Firearms and Explosives). Our discussion of federal efforts was covered in the earlier literature review. The focus of our research was local practices.

The section that follows provides a description of what our team (and the experts we consulted) felt were promising practices in port security. The data to compare which were the best among these promising practices were just not available. We believe it would be misleading to offer a prioritized list. Each port will need to consider our results one-by-one and assess their relevance to their port, given their own local conditions and circumstances.

For clarity, the practices have been categorized according to the nature of their contribution to the various components of the National Strategy for Maritime Security (2005):[23]

- Awareness;
- Prevention;
- Preparedness;
- Response; and
- Recovery.

Awareness

Awareness is the continual process of collecting, analyzing, and disseminating intelligence, information, and knowledge to allow organizations and individuals to anticipate requirements and to react effectively. Awareness of an adversary's capabilities, intentions, methods, objectives, goals, ideology, and organizational structure, plus factors that influence his or her behavior, is critical for securing the maritime domain[24]. The idea is that domain awareness will enable the early identification of potential threats and facilitate appropriate responses, including interdiction by the U.S. government at an optimal distance with capable forces.[25]

Achieving awareness of the maritime domain is challenging due to the size of port areas, the lack of complete transparency into the registration and ownership of vessels and cargoes, and the fluid nature of the crewing and operational activities of most vessels. Domain awareness requires integrating all-source intelligence, law enforcement information, and open-source data from the public and private sectors; it is heavily dependent on information-sharing and requires unprecedented cooperation among the various elements of the public and private sectors[26]. To maximize domain awareness, some of the port officials we talked with are attempting to leverage the intelligence capability of the U.S. government and the diverse expertise of the intelligence and law enforcement communities. However, challenges remain in implementing a shared situational awareness capability that integrates intelligence, surveillance, reconnaissance, navigation systems, and other operational information inputs, combined with access at multiple levels throughout the United States government (see Haveman and Shatz, 2006).

Across our set of study ports, a number of measures have been used for some time, or have been established recently, to increase awareness of threats to acts of terrorism at seaports.[27] We have grouped these into two main efforts: (A) stakeholder coordination and collaboration initiatives, (B) protocols and systems for detecting and monitoring port-related security risks/intelligence sharing. Below we discuss a number of systems, programs or initiatives that fall under one of these two areas.

Stakeholder Coordination and Collaboration Initiatives: Area Maritime Security Committees

A primary form of awareness of port security issues came from the sharing of information by stakeholders in the port communities. The most notable "promising practice" in this realm is the Area Maritime Security Committee (AMSC) called for by the Maritime

[23] Some of the programs could legitimately be considered in more than one category. In these cases, we have placed the initiative according to its most dominant feature.
[24] See http://www.whitehouse.gov/homeland/maritime-security.html.
[25] See http://www.whitehouse.gov/homeland/maritime-security.html.
[26] See http://www.whitehouse.gov/homeland/maritime-security.html.
[27] Some of these measures also have prevention components.

Transportation Security Act (MTSA) of 2002. AMSCs are tasked with collaborating on plans to secure ports so the resources of an area can be best used to raise maritime awareness of terrorism and to deter, prevent and respond to terror threats.

Under this act, the Coast Guard, in the person of the Captain of the Port, creates a committee—made up of representatives of federal, state, local, and private sectors—to identify and deal with vulnerabilities in and around ports, as well as to provide a forum for sharing information on issues related to port security. In all, the Coast Guard ultimately organized 43 AMSCs. Although AMSCs existed at all ports visited by the evaluation team, the groups varied considerably in terms of the size of membership, the types of stakeholders represented, the frequency of convening, and the methods of functioning. For example, to prevent duplication of efforts, some of the committees rely on existing information-sharing networks, such as trade and industry associations, and have Coast Guard officials participate directly with these groups.

Houston/Galveston AMSC. This AMSC evolved from the East Harris County Manufacturers Association (EHCMA) and the Houston/Galveston Navigation Safety Advisory Committee (HOGANSAC). The EHCMA is a trade association of more than 125 refineries, petrochemical plants, and storage distribution facilities. HOGANSAC was created to provide advice and consultation to the Coast Guard on issues of concern in the Houston-Galveston-Texas City region. Its 19 members include a variety of waterway users, including pilot associations, shallow draft interests, deep draft operators, environmental interests, and academics. The committee discusses, researches, and makes recommendations on a wide range of topics, including safety and security. Other individuals are called upon to participate in working groups created to deal with specific problem areas. In November, 2001 HOGANSAC established a Port Security Subcommittee, which eventually became the Houston-Galveston AMSC, containing representatives of all the legacy agencies as well as several more from the ports of Houston, Galveston, Texas City, and Freeport. The AMSC has a website that posts security bulletins and suspicious activity report forms, describes security zones, and offers other relevant material.

*Charleston AMSC***.** This AMSC was created by building up the Maritime Association of the Port of Charleston, a trade association created to promote the interests of the Port of Charleston in 1926. The Captain of the Port turned to this group to serve as the core of the AMSC. Officials of the Coast Guard and other federal and local agencies have joined the association and use the regular meetings as one way of sharing information with stakeholders. An important aspect of this particular AMSC is that it has a separate intelligence subcommittee made up of members who have security clearances.

Jacksonville AMSC. This AMSC (known locally as the Port Security Committee) is coordinated by the Jacksonville Marine Transportation Exchange, a maritime trade organization created to "coordinate the safe, secure and environmentally responsible management of the marine transportation system within the port of Jacksonville." The Exchange includes representatives of the major port stakeholders. To that base group, the AMSC adds representatives of the port as well as law enforcement officers from local and state agencies.

Port of Savannah AMSC. This AMSC was assembled shortly after 9/11 and is made up of all the major law enforcement agencies and members of the business community in the Savannah area: the U.S. Customs and Border Protection, the Coast Guard, the Georgia Bureau of

Investigation, the Savannah/Chatham Police Department, the Georgia Port Authority Police, the Savannah Maritime Association, chiefs of two local tug boat companies, and the Savannah River Pilots. This committee meets regularly to work on port security planning issues, communicating among stakeholders, sharing intelligence, and planning for tabletop exercises. The full committee of more than 100 members meets annually, and various working groups meet more often.

South Puget Sound Port Security Committee (SPSPSC). The Ports of Seattle and Tacoma are part of the SPSPSC**.** The SPSPSC consists of a large number of key stakeholders that include: the Coast Guard Marine Safety Office, Puget Sound; Seattle, Tacoma, Everett and Olympia port authorities; federal, state, and local law enforcement; the Department of Defense; federal, state, and local regulatory compliance agencies; port tenants; carriers and shippers whose vessels, vehicles, cargoes, and passengers use the port; and vessel and port tenant servicing organizations and agents. The committee provides a Steering Committee and a General Port Security Committee with workgroups, open to all port security stakeholders. The mission of this committee is to help coordinate planning, information sharing, and other necessary activities to enhance the security of the marine transportation system (MTS) within its area of responsibility. In support of this mission, the committee is developing a Port Security Plan which outlines scalable security procedures to be taken by MTS stakeholders to ensure the continued safety and security of the South Puget Sound port facilities and MTS.

Programs, Policies, and Procedures that Identify and Analyze Security Risks/Intelligence Sharing

In addition to the Area Maritime Security Committees, several ports have created other methods by which they can share information and intelligence. Some of the most promising of these approaches are summarized below.

Boston--Daily security briefings. At these briefings, the Port of Boston invites local, state, and federal law enforcement, as well as representatives of private industry, to discuss information that might be relevant to security at either the port or Logan airport.

Boston-- State Fusion Center. This center is run by the Massachusetts State Police and is tied into the federal information-sharing network. The Fusion Center collects and shares intelligence information concerning terrorism and transportation with all Massachusetts law enforcement agencies. This information is shared at all port police roll calls.

Boston--The Joint Terrorism Task Force (JTTF). The JTTF sends out e-mails containing important terrorist-related information. The JTTF also provides a daily web board with pertinent information.

Charleston--Daily meetings. These meetings involve all relevant local and federal agencies involved with port security to discuss possible security threats and to plan countermeasures and response.

Charleston--Project Seahawk (see fuller discussion below). Charleston has an intelligence unit that involves intelligence officers on assignment from several local, state and federal agencies. This unit collects and analyzes intelligence information that may affect port security. Seahawk representatives have reached out to dive shops, marinas, hotel operators and others to inform them of the importance of identifying possible terrorist suspects and the need to convey that information to law enforcement officials.

Charleston--Voluntary Port Security Force. This is an organization of local persons interested in port security who operate as a "neighborhood watch" to alert law enforcement concerning suspicious behavior. They produce a quarterly newsletter to keep members apprised of recent developments.

*Charleston--The South Carolina Naval Militia***.** This group is comprised of Navy reservists who provide information to authorities concerning suspicious activities.

Charleston--Yard Management System (YMS). This is an excellent example of a system that provides a high level of integration between security and operational data. The YMS is a proprietary container yard computer management system that allows the port to maximize use of existing facilities through automation, increase container throughput volumes, and improve reporting and billing processes. The YMS allows the Port of Charleston to implement consistent port operations at all container terminals with electronic controls and reporting. The YMS is an excellent aid for enhancing security at the port by allowing the tracking of all cargo into and out of the port and all the equipment used for moving the cargo. YMS provides real-time data on the location of each piece of equipment—where a chassis is, which box goes on the chassis, which boxes are booked to each ship scheduled, where each box is, and all the data associated with the movement of that equipment. YMS essentially plays traffic cop with every box and chassis in the port.

Houston--Port Intelligence team. This team was created in 2002 and is coordinated by the Coast Guard. The team is made up of representatives from the FBI, ATF, U.S. Naval Intelligence, U.S. Army Intelligence, Secret Service, FBI, CBP, the Texas Department of Public Safety, the Houston Police Department, and the port police. This group meets regularly to discuss current intelligence about port security issues. Discussions are limited to cleared personnel. A Law Enforcement Work Group serves as a subcommittee of this group, charged with the task of carrying out specific tasks requested by the Captain of the Port.

Houston-- Law Enforcement Subcommittee. This subcommittee is a part of the Area Maritime Security Committee of Houston, and was created by the Captain of the Port to respond to specific challenges and tasks related to law enforcement at the Port of Houston.

*Houston--Anti-Terrorism Advisory Council***.** This council was formed by a U.S. Attorney under the auspices of the Patriot Act. It brings together representatives of law enforcement, private industry, private security, schools, hospitals and others to identify security-related issues.

Houston--FBI's Counter-Terrorism Intel Group (CTIG). CTIG includes analysts from many local law enforcement agencies, who analyze threat data and supply their analyses to the Joint Terrorism Task Force.

*Houston--The Texas Security Alert and Analysis Center (TSAAC)***.** TSSAC is the Texas Fusion Center, the central facility for collecting, analyzing, and disseminating information related to terrorist activities. This Fusion Center is integrated with the State Operations Center of the Governor's Division of Emergency Management at the Texas Department of Public Safety. The center is designed to receive and respond to Internet and telephone inquires from the general public and other law enforcement agencies.

Houston--The Energy Security Council. This council is comprised of security managers of petrochemical companies in the Houston area. It meets quarterly to discuss common security concerns.

Houston--Coast Guard auxiliary. Members of the auxiliary are used to inform recreational boaters and fishermen about security zones that are off-limits to them. In their

dealings with the public, the auxiliary also stresses the importance of providing any security-related information to authorities.

Houston-- JTTF Terrorism Intelligence Summary. The local JTTF issues a weekly Terrorism Intelligence Summary (containing non-classified information) to all command staff and mid-managers in local law enforcement agencies, as well as to the Coast Guard, the Department of State and other concerned actors.

Jacksonville--Joint Terrorism Task Force. The local FBI JTTF works closely with both the Jacksonville Sheriff's Office and the port security office to ensure an ongoing dialogue of intelligence information.

Jacksonville--Northeast Florida Domestic Security Task Force. This task force is one of seven such groups created by the Governor of Florida to coordinate state and local policies and plans to defend against and respond to terrorist attacks. Each task force is organized under the Incident Command model and is co-chaired by a regional director of the Florida Department of Law Enforcement and a local sheriff. Membership includes police chiefs, fire chiefs, emergency management directors, health and medical officials, private industry representatives, and government officials from the federal, state, and local levels. One of the major responsibilities of the task force is to detect and prevent potential terrorist threats by collecting and disseminating intelligence and investigative information. The group also promotes public awareness of how suspicious incidents can be identified and reported, to improve the area's response and recovery capabilities.

Los Angeles--Regional Terrorism Threat Assessment Center (RTTAC). RTTAC is one of four fusion centers throughout California; the others are in San Francisco, Sacramento, and San Diego. The RTTAC is managed and staffed by local law enforcement, fire services, and other public safety agencies that maintain close, cooperative, coordinated, and mutually supportive working relationship with each other, the FBI Joint Terrorism Task Force, and the State Terrorism Threat Assessment Center. The Center receives and analyzes intelligence concerning possible terrorist threats and disseminates information to appropriate regional stakeholders.

*Los Angeles--Joint Regional Intelligence Center (JRIC)***.** JRIC opened in late 2006. JRIC is a multi-agency fusion center designed to analyze and compare intelligence information from various sources in order to identify and interrupt potential threats to the safety of the Los Angeles region. The first of 38 such centers, the facility houses analysts from the FBI, the Los Angeles Police Department, the Los Angeles Sheriff's Department, and the Department of Homeland Security. The analysts, experts in such diverse fields as biological contamination, hazardous materials, and terrorist tactics, communicate with more than 200 agencies, including the Port of Los Angeles.

Los Angeles--County Terrorism Early Warning (TEW) Group. This group was created in 1996 in response to threats from Osama bin Laden, who had just issued his first fatwa urging his followers to conduct global terrorist attacks against the United States. The group was initially formed by the Los Angeles Sheriff's Department, the Los Angeles Police Department, the law enforcement branch of California's Office of Emergency Services, and several academic and research institutions. Later the group added representatives from the FBI, city and county fire services, public health, public works, and local law enforcement agencies. The purpose of the group is to monitor and assess intelligence concerning terrorist threats, identify trends, develop a coordinated response to incidents, and disseminate information to incident commanders in the

case of actual incidents. The Port of Los Angeles assigns a Terrorism Liaison Officer to support the TEW and uses that contact to maintain current information about threats.

*Los Angeles--Port Community Advisory Committee***.** This committee is made up of neighborhood organizations in regions surrounding the port. The Committee serves as a forum for port representatives to relay information (some of which is terrorism-related) to residents in the port community and to elicit information from them as well. As with other Los Angeles groups listed above, this committee works in close collaboration with the FBI's Joint Terrorism Task Force and Field Intelligence Group (made up of intelligence analysts, special agents, language analysts, and surveillance specialists). They also work closely with the Coast Guard's Field Intelligence Support Team (FIST).

New Orleans--The Louisiana Anti-Terrorism Advisory Council (ATTC). ATTC is one of 93 such councils (previously called Anti-Terrorism Task forces) created as a result of a directive issued by Attorney General John Ashcroft in September 2001 to the United States Attorneys. The directive stipulated that councils be created, comprised of federal, state, and local law enforcement agencies, which would work with the 66 Joint Terrorism Task Forces (JTTFs) to ensure that law enforcement focuses on terrorism. While the JTTFs retain primary responsibility for terrorism investigations, the ATTCs implement prevention-based initiatives and provide a forum for agencies to identify potential terrorism links among their investigations. In addition, the Councils are responsible for initiating training programs and facilitating information programs. The New Orleans Port Police maintain regular contact with the Louisiana ATTC, which meets monthly.

New Orleans--Urban Area Security Initiative (UASI) Group. The UASI for New Orleans is chaired by the New Orleans Director of Homeland Security, and among other things serves to coordinate anti-terrorism efforts for New Orleans agencies. The Port Police also work closely with this group.

Port Everglades--Daily security meeting. A daily meeting is convened involving representatives of the Broward County Sheriff's Office, the port authority management, the Coast Guard, the Florida Department of Law Enforcement, and others concerned about port security to discuss potential security threats and to coordinate responses.

San Diego--Regional Information Sharing and Analysis (RISA) project. RISA, also known as the Pre-Incident Indicator Project, is a multi-jurisdictional data-sharing and analysis project that uses a wide range of data (including field interrogation reports; arrest reports; calls for service; and vessel, cargo, and crew information) in order to provide an intelligence/predictive analysis capability to assist in preventing terrorist incidents. Data are provided by the San Diego Harbor Police, the San Diego Police Department, the Los Angeles Port Police, the Long Beach Police Department, and the U.S. Coast Guard. The system can identify patterns and trends of events, clusters of suspects, similarities of crime modalities, and other configurations.

San Diego--Harbor Police Homeland Security Unit. This unit has been charged with coordinating community outreach and public awareness campaigns to make port tenants, marina residents, hospitality workers and others more aware of the nature and indicators of terrorist activities and how to report them.

San Diego--Terrorism Early Warning (TEW) Group. This group functions in San Diego in much the same way as the equivalent group does in Los Angeles. (See description above.)

Savannah--The Georgia Fusion Center. This center functions here in a way similar to that of other fusion centers, such as those in Los Angeles and Houston (see discussions of those sites).

Savannah--Navis WebAccess system. This system gives key stakeholders in the port/terminal community access to pertinent terminal transaction information. Navis WebAccess is a self-help tool that allows customers and security personnel to access real-time container information, reports, appointment management, and automated event notification, while reducing the workload for port staff. Navis WebAccess enables the Port of Savannah to accomplish many business transactions with its terminal customers online, through a standard Web browser, and to keep updated as containers arrive and move through and leave the gate. While designed to improve the flow of commerce, this system is heavily used by the Georgia Port Authority police to address security concerns.

*Seattle--Washington State Ferry Security Committee***.** This committee provides oversight over security operations on Washington State ferries.

Seattle--MPS/ATLAS technology. This system allows complete and continuous container-to-container, container-to-logistics center (via satellite or GSM), logistics center-to-container, and logistic center-to-authorities and customers asset monitoring and tracking. In addition to providing total supply chain visibility, with early loss and damage detection, the MPS/Atlas technology provides a means of mitigating potential security threats to people and property at the Port of Seattle.

Tacoma--Maritime Intelligence Support Team. The non-commissioned Port Security Service has created a Maritime Intelligence Support Team that produces three types of intelligence reports concerning port security: 1) a situation analysis report for agency supervisors, 2) an information bulletin for intelligence officers, and 3) a biweekly activity analysis sent to federal, state, and local law enforcement agencies.

Tacoma--Central Point of Coordination Rail Management System. This system is a promising practice in the area of rail security and linking security data with operational data. In 2002, the Port of Tacoma invested in a series of Automated Equipment Identification (AEI) sensors and other infrastructure to collect rail-car and container data. These data are displayed and analyzed via proprietary application software called "Signal AEI Manager." This system has since been supplemented by a Web-based solution that improves the port's ability to disseminate this information to a larger number of users and interested parties. The solution, called "Central Point of Coordination Rail Management System," was developed for the purposes of decision support visualization and data display, as well as management, planning, and facilitating operational analysis. This system gives stakeholders internal and external to the Port of Tacoma a gateway to rail-car and container information via the Internet. This combined sensor, visualization, and mapping system has not only been designed to support the day-to-day operations of the Port of Tacoma rail yard, but is also used as a safety and security support tool in the event of either natural disaster or act of terrorism.

Tampa--Daily security e-mail or telephone conferences. These emails and conferences involve the Hillsborough County Sheriff's Office, the Coast Guard, CBP, and the Florida Department of Law Enforcement, and include discussion of developments in port security, including suspicious activities, outstanding warrants, and recent intelligence. At the time of the evaluation site visit, plans were being made to include private security and facility security officers.

*Tampa--Port Watch***.** A port watch has been implemented, similar to neighborhood watch, in which tenants in the port disseminate information to each other concerning security concerns. A phone tree allows messages to be disseminated throughout the port community.

Tampa--Regional Florida Domestic Security Task Force. This task force is one of seven such groups created by the Governor of Florida to coordinate state and local policies and plans to defend against and respond to terrorist attacks. (See the discussion under Jacksonville above.) As in Jacksonville and other Florida ports, this task force plays a critical role in coordinating port security.

Texas City--Port Security Council. The port formed a Port Security Council, made up of representatives of each of the tenant companies, to provide intelligence and advice concerning security issues. This is separate from the Area Maritime Security Committee.

Prevention

Prevention involves efforts taken to intervene to stop an incident from occurring. This can involve measures such as creating physical barriers, limiting access, installing detection equipment, increasing law enforcement efforts, and coordinating efforts among relevant agencies. The Maritime Transportation Security Act requires that all ports improve perimeter security and access control, and has provided funding, through Port Security grants, to implement many of these changes. Other improvements have been made or are being made more at the discretion of local authorities.

The idea behind the concept of prevention and "target hardening" is that a strong, visible defense will deter or delay an attack. It is similar to the concept of opportunity reduction, except that what matters is that security measures should be visible in order to send a clear message or signal. Target hardening is part of the field of Crime Prevention Through Environmental Design (CPTED), where it has enjoyed some success in preventing burglary and robbery. In the context of ports, target hardening is the process of making a port a more difficult or less attractive target. It does not necessarily mean that a target is impenetrable. For example, the use of "smart" or "tamper evident" containers has increased security for containerized shipping. This technology is designed to leave evidence that someone has attempted to open a container, not to make the container impenetrable

In this section we cover five categories of prevention activities: (1) physical security/infrastructure at seaports, (2) protocols and processes limiting entry to seaports, (3) technology detection/inspection systems, (4) law enforcement-related activities, and (5) interagency operational centers.

Physical Security/Infrastructure at Seaports

There are a number of ways to do target hardening to secure the outer and inner perimeters of a port. Outer-perimeter defenses consist of items such as barriers, fences, walls, gates, locks, lighting, surveillance, roofs and walls, and landscape design and zones. Inner-

perimeter defenses consist of doors and pass systems, files and information technology systems, safes and vaults, inspections, and alarms. Many ports also include the building interior within their target-hardening plans, controlling access to port administrative buildings and lobbies, utilities (generators, fuel systems, sprinkler systems, water supplies, heating, ventilation, air conditioning, and air filtration systems), windows, elevators, stairwells, and security control centers.

Perimeter security (Land-based security, fencing and other restrictions). As mentioned above, the MTSA required ports to increase their perimeter security. As a result, all of the ports visited by the evaluation team have either installed perimeter security measures or improved existing devices. Because of the size and complexity of many ports, this required that they first designate restricted areas and/or security zones. In some cases, such as San Diego and Boston, numerous non-marine facilities, such as hotels, office complexes, and convention centers, are located on port property. For practical and security reasons, most of these non-maritime facilities have not been designated as secure areas. Areas with access to shipping, however, are required to have strict perimeter measures and improved access control.

One of the basic forms of perimeter control is the use of a fence. Regular fences can be easily circumvented. However, security enhancements can be added to make it more difficult to get past a fence. We observed a number of these enhancements during our site visits. First, barbed wire is commonly integrated onto the tops of fence lines to deter scaling. Also, installation of barbed wire along the bottom of the fence line can deter efforts to gain access underneath the fence and act as an additional deterrent to fence climbing. Next, the fencing surrounding the port facility perimeter can be set in concrete. The concrete makes it very difficult for anyone trying to gain access by digging under the fence line to gain access. We also observed the use of fencing to support security for seaport-related rail systems. Trains and railroad tracks entering port facilities present a number of security issues for facility managers and security officers. Some port facilities address train security issues by installing a gate that is closed and locked across the tracks when no train is expected, and by posting security guards at the entrance when the gate is opened to permit a train to pass. The security guards can look for unauthorized persons or materials concealed on the train. Procedures can also be established to inspect the undercarriage of entering and exiting trains for unauthorized persons or materials.

The MTSA law has required all ports to install fencing around restricted areas. Some examples are provided below.

In Boston the port obtained grant funding to heighten the perimeter fence (beyond federal requirements) and upgrade the barbed wire on top with a spiked device. In Galveston the port enclosed the west end of its property and installed a security gate. In Houston the waterfront has been fenced, and turnstile gates for employees were installed. In Miami, fencing has been added to separate cruise terminals from cargo areas. In Savannah, electronic locks have been placed on railway entrances to the port, making it difficult to force them open. Video coverage is also visible from the port's command center. The ports in Tampa and Texas City had no perimeter security before 9/11. Since then, all MTSA requirements for fencing, access control, and other security measures have been met.

At a waterfront facility, a common challenge to the effectiveness of walls and fences is the land/water interface, because it can be difficult to prevent intruders from climbing around walls and fences at the waterline. This is especially problematic with tidal water, which rises and recedes, often leaving a gap at the end of the fence during low tide. This issue can be addressed by continuing the construction of the fence from the land down into the channel, so the fence

creates an effective barrier against intruders regardless of the tide level. Lateral supports can be used to protect the fence against tidal movement. For certain applications, especially those involving relatively still water, this can be an effective approach. This type of fence would not likely be effective in fast moving (river or fast current) water.

Another approach to the problem of restricting waterside access to port facilities is the use of infrared motion detection devices along the waterside perimeter. The infrared beam is installed so that it is almost impossible to crawl underneath or jump over it. An activation of the infrared motion detector will alert security to the section of the perimeter alarm that was activated. One of the concerns with these systems is that they can be accidentally activated by large birds or other wildlife, causing multiple nuisance responses, which can cause security to ignore an activation by an intruder. However, some of the port security experts we consulted felt that the infrared motion detection system can be effective when used in conjunction with other security measures and can fill in the gaps left by fencing and patrols.

Another security feature that can be added to fencing is an anti-passback feature at security gates. With this system, an ID card will activate electronic entrance and exit gates and doors to the facility only once per day. If a card is used and then "passed back" to another person through a gate or under a door, the card will not activate the gate or door a second time. Employees who find a need to re-enter an area must either go to security personnel to have the access control system reset, or can stand in front of a facility CCTV camera and call security to request a second access. If an electronic lock system is already in place or planned, the additional cost to program in an ID Card anti-passback feature should be minimal. To be effective, an anti-passback system needs to be part of a larger centralized access control and CCTV monitoring system.

Another perimeter security measure, when fencing is not enough, is the use of concrete anti-vehicle barricades--sometimes called "Jersey barriers." These types of barriers are highly effective at stopping vehicles. In the event of an elevated threat level, these barriers can be used to close the facility entrance. The barricades are relatively inexpensive to purchase. Concrete barriers are a low-cost, high-value protective feature that can be used in many ways to protect sensitive or valuable elements in a port, both outside and inside the perimeter gate. For example, concrete barriers may be placed around emergency generators to prevent a terrorist from disabling the port's emergency power source. And concrete barriers placed behind a fence line can provide protection against a vehicle ramming and knocking down a fence.

Other types of anti-vehicle measures include caltrops and spike-strips. These low-cost vehicle barrier devices can be constructed from scrap steel. Small caltrops and spike strips work by causing tire blow-outs of vehicles that are driven over them. Large caltrops roll under a vehicle, raising the front wheels off the ground and causing the driver to lose control. These vehicle barriers can be used to enhance security at any access point where vehicles or motorcycles can gain access to a facility. The devices can be easily positioned in front or behind of existing gates or fence lines. The devices can be produced in large numbers and placed on exterior roads or parking lots to expand the perimeter of any port facility during heightened security levels. The devices can be used at any facility and require minimum training for proper use. These devices can be easily mass-produced by any welding facility with access to steel stock or scrap metal, and can be easily deployed by security personnel.

Sea-borne security devices--floating booms and barriers. Our team observed innovations in this area in Boston and Port Everglades. In Boston, floating barriers are now being used

around cruise ships and LNG tankers when they are in port. Also, in Boston, stores for cruise ships are sent for X-ray and Radiation Portal Monitor inspection away from the cruise terminal. Once determined to be secure, trucks are escorted to the terminal where the stores are loaded onto the cruise ship. Explosive-detecting dogs may also be used. In Port Everglades, portable floating booms are used around cruise ships when they are docked in the port to protect against sea-borne attacks.

Lighting. Virtually all of the ports our team visited have installed additional lighting, both on the port perimeter and throughout the facilities. Lighting is important not only for security but also for safety in nighttime loading operations. The ports we visited have worked to increase lighting of docks, container traffic, and storage areas. The better security operations had clear illumination of all facility areas, perimeter fence lines, entrances, exits, cargo holding areas, piers, harbor and harbor approach, ship's waterlines, gate houses, and emergency lighting for assisting in fire suppression and evacuation.

A good example of an expansive lighting system is in place at the *Port of Texas City*. Some port facilities there maintain two tiers of outdoor facility lighting; regular outdoor lighting on 12 foot poles, and high-intensity 50-foot light towers. During normal operations the facility only uses the regular outdoor lighting to provide working illumination during hours of darkness. During heightened security risk levels, the facility can use the high-power light towers to brightly illuminate the facility to daylight conditions. This type of configuration can save energy by not using unnecessary lighting during normal operations or when there are no vessels at the facility.

In some ports, light towers also serve as guard towers. Lighting towers can be built with elevated platforms that permit guards or port officials to climb the towers and observe the port, adjacent waterways, and surrounding area from an elevated position. Mobile light towers are in place in some seaports and can be positioned as needed to provide supplemental lighting on the port. A mobile diesel-powered light tower provides the mobility to quickly move lighting to areas of specific temporary concern, threat response, or cargo operations, as well as the ability to provide effective lighting during power outages affecting other facility lighting. In event of repair operations on perimeter fencing, a mobile light tower can illuminate temporarily unsecured areas, deterring trespassers and improving the ability to detect them. For facilities without reliable backup power for their security lighting, or where intermittent lighting needs or other security needs exist, a mobile light tower can be highly effective at improving lighting and facility security.

Other lighting innovations include using solar-powered emergency street lights to supplement port security lighting in event of a power outage of the primary and secondary power sources.

*Door-to-door stacking of empty shipping containers***.** One simple strategy used by most of the ports we visited was door-to-door stacking of empty shipping containers. While not a foolproof system, stacking containers door-to-door is a very simple method of limiting either terrorists, stowaways or smugglers with contraband from gaining entry into shipping containers, as well as helping to prevent thieves from stealing the contents of shipping containers. Under this system, empty inter-modal shipping containers are sealed in the port in the presence of Customs officers, then stacked door-to-door (back-to-back) to prevent unauthorized access. This simple change in container storage procedures can increase port, cargo, and homeland security by

reducing theft as well as the number of stowaways or amount of contraband leaving a country in empty containers. This system should involve only a small investment of time to train dock employees and plan container movements accordingly.

Protocols and Processes Limiting Entry to Port/Secured Areas

We observed a number of promising protocols and practices that have been established to limit entry to seaports, including: improved access control, the use of new technology detection/inspection systems, changes in law enforcement, and the use of interagency operational centers.

Access control (security gates/guards, employee identification, background checks). Although seaports have historically used more conventional forms of access control such as ID badges, the increased focus on seaport security is driving the Department of Homeland Security, the U.S. Coast Guard, and port commissioners to promote the use of a national credentialing system for seaport workers, as well as technology-intensive access control systems. The emergence of the Transportation Worker Identification Credential (TWIC) will transform access control throughout U.S. seaports, making comprehensive data capture, cost-effective storage and archiving, and efficient integration and sharing of data crucial operational priorities for ports. Accordingly, seaports are turning to multiple types of access control devices to control entry of seaport personnel into dock and cargo areas. The development of biometric controls, including facial, retina, iris, fingerprint, and hand geometry scans, has opened up opportunities for more robust analysis and tracking across the supply chain and in intermodal operations. Utilizing storage networking technology that maintains ready access to data also expedites the verification process at access points, reducing traffic congestion and long lines at port access points.

In addition to high-tech solutions, some ports have instituted simple measures to help control access to the port. For example, some ports have worker identification numbers stenciled on their port-issued work clothes. Port workers are required to wear these clothes, and the clothes are color-coded to identify the type of work and position the employee holds. A worker's identification number appears in large bold print on the back of his shirt or jacket, which can be clearly read by personnel monitoring security cameras. Both color-coded and stenciled work clothes provide a good, low-cost method for helping assess who should and should not be present in the port facility and in various work areas.

Many U.S. ports are turning to technology to improve safeguards not only on the cargo that flows in and out of ports, but increasingly, the people as well. In fact, the MTSA requires that ports institute a range of protocols and processes to limit entry to seaports, and to control access to restricted areas in their facilities. Some examples are summarized below.

In *Boston* the port police have been conducting random searches of sleeper cabins, vehicle undercarriages, and empty containers. Parking has been prohibited inside secure areas. Only line handlers in a company truck or van can go on the dock in the Port of Boston. Access is programmed into an ID card. Visitors to the Port of Boston must provide the name of the person being visited and the reason for the visit. The person being visited must be contacted for verification. Electronic ID cards (for employees, tenants, and longshoremen) have been distributed and are required to enter and exit the port, as well as enter other secure areas. For visitors, grant money has been used to purchase devices to verify the legitimacy of driver's licenses and passports, and to check names against the DHS watch list.

In *Charleston* employees must have an appropriate ID card with a badge and vehicle decal for access to the port. Vehicles are randomly inspected to determine if they have dangerous

materials or unqualified persons. Also, longshoremen are expected to park in a lot away from the dock and take buses to their work area (see more detailed discussion of shuttle buses).

In *Galveston* the port authority has issued a port ID card to all employees, tenants, and users. Visitors to the port also have to articulate a reason for visiting the port and have a contact person.

In *Houston* the port authority has instituted ID cards for employees and terminal workers, with proximity card capabilities and fingerprint readers; this allows access to only certain areas at designated times. Access to the waterfront is restricted, as it is to certain facilities. Employers in the port must submit official letters of endorsement to verify that employees deserve and require ID badges. Employees are required to park in off-waterfront areas. The port has also purchased document verifiers that determine if driver's licenses and/or passports are valid. Tenant leases have been written to require employees to pass background checks.

In *Jacksonville, Miami, and Port Everglades,* Florida legislation, passed in 2000, required the creation of a computerized identity card for all employees and others using the port. This card is available to those who successfully pass a fingerprint-based criminal history check. Anyone found guilty within the preceding seven years of any of several felonies is deemed ineligible. This Florida Uniform Port Access Credential Card (FUPACC) is required for any individual working within or authorized to regularly enter a restricted access area in any of Florida's 14 major ports. This FUPAC card preceded and in many respects served the model for the federal Transportation Workers Identification Credential (TWIC), soon to be required by the Transportation Security Administration and the U.S. Coast Guard.

In *New Orleans,* grant funds have been received to install a new employee ID card system. Also, in *Savannah,* the Georgia Ports Authority has instituted a smartcard-based credentialing system, requiring all persons employed by or doing business on the port to have an authorized credential. The Port of Savannah also has instituted a computerized system to track operators and shipments coming into and exiting the port. This allows the port to determine who is on the port, and where, at any given time.

Finally, *Texas City* requires all persons seeking access to the port to have an ID badge issued at a security command center that was created after 9/11. The Port of Texas City has also implemented an impressive computer-based access control system that regulates the entrance to and around the port premises.

As mentioned above, some port facilities are now requiring personnel working or visiting the facility to travel between facility areas on a facility-owned and -operated shuttle bus. For example, in some *Port of Jacksonville* terminals, employees must park outside and take a bus to waterside. No personal vehicles are allowed on the pier in the Port of Jacksonville. The *Port of Charleston* has a similar shuttle bus system.

A shuttle bus can provide several benefits to a port facility. It is a means of limiting pedestrian access to unauthorized areas and limiting random foot traffic around the facility. Certain facility areas can only be accessed via shuttle bus, and the shuttle bus driver can be authorized to check employees' ID tags for area access authorization before allowing them to enter the area. Also, the shuttle driver is performing a constant roving patrol on the facility. The driver is aware of normal facility operations and personnel, and if trained properly and equipped with a radio, the driver can report suspicious persons, vehicles, or activity. A shuttle also eliminates the need for many employees to drive their vehicles on the facility. Employee vehicles can be parked outside the facility, limiting the security risk and congestion associated with having employee vehicles inside the facility. The shuttle can also limit the potential for injuries

to pedestrians from facility vehicles racing around blind corners. The shuttle also provides a benefit to employees not inclined or able to walk around the facility, increasing employee efficiency and job satisfaction.

However, the cost to purchase, maintain and staff a shuttle bus can be considerable. And in small facilities with fewer than 100 employees, a shuttle would typically not be efficient. Also, as we learned on some of our site visits, port personnel tend to prefer the convenience of parking on the port facility and operating their own vehicles. Therefore, steps would need to be taken to reach out to various port personnel and unions/employee bargaining groups to explain why the shuttle is being established and the importance of having their support in using the shuttle system.

Technology detection/inspection systems. A great deal of attention is focused on the development of the next generation of closed-circuit televisions (CCTVs) and sensors to detect chemical, biological, radiological, and nuclear weapons of mass destruction. Seaports are deploying numerous technologies to secure the complete spectrum of seaport operations and physical assets. These systems have great potential, especially when used in combination with traditional security practices.

The use of CCTVs at seaports is highly prevalent. However, seaports present a number of challenges for CCTVs in that much of a port's perimeter is water without physical barriers. Since small boats in gusty seas are very difficult to detect, generally a combination of technologies is used to supervise these areas and detect wrongful approaches. Many seaports are shifting to what was described to our research team as an airport model, where a single graphical-user interface handles all access-control, CCTV, DVR, and video-analytics requirements from a central head-end location. Early seaport installations had rather unsophisticated yet expensive camera deployments. Now, manufacturers such as Honeywell have begun to offer port-specific software and hardware platforms that greatly reduce both installation and operational costs by combining multiple technologies onto one easy-to-use screen, so less training, user interface, and system knowledge are needed to properly respond to potential threats and vulnerabilities.

Too many cameras, continuously moving, can be distracting to the guard or police officer monitoring the cameras, and can possibly cause him to miss something happening on one screen. This can be moderated by ensuring that a guard is not required to view too many camera images at one time, and/or adjusting the speed of the computer algorithm so the pictures don't move too quickly. Also, a number of CCTV systems employ computer algorithms that continually move multiple pan/tilt/zoom (PTZ) cameras in a pattern covering the range of each camera so the security specialist at the console can view the entire port area without manually moving each camera with a joystick.

Some of the better systems we observed combine CCTV and video analytics. Video systems deployed around the harbor and port areas are combined with video analytics software algorithms to analyze video proactively based upon behavior. Rules are then established to guide operators on when to respond to perceived threats or anomalies.

For instance, a port can set up virtual fencing around an area displayed via geospatial maps of the port on a graphical interface. If vehicles or boats travel within this predetermined area, an alarm is immediately generated, an operator is notified, and video is recorded. This process occurs simultaneously, with very little, if any, user interaction (other than assessment) required. Another example is the ability of video analytics to notice behavior, such as a person carrying a briefcase who sits down and then walks away from the immediate area. This behavior,

based upon rules selected by the port, triggers an alarm and the same process described above. Video analytics require a high number of cameras to make proper assessments; this can prove budget-intensive for ports with little or no proper communications infrastructure. Video analytics are important because ports have continuous motion, so simple motion detectors cannot be used. Rather, such devices must determine unusual behavior, such as a ship or vehicle stopping in the wrong place or moving in an inappropriate direction.

Next, a great deal of scientific attention is focused on the development of the next generation of sensors to detect chemical, biological, radiological, or nuclear weapons of mass destruction. One very promising practice is the use of sensor technologies to serve as screeners. As with many technologies, these sensory devices can be helpful, but there is still no technological substitute for good security procedures and well-trained human inspectors. Also, a major challenge in deploying many of these technologies at a port facility is the communication infrastructure; most ports were never designed to move video and data communications from one side of the facility, harbor or perimeter to the other. Ports also present major technical challenges because cameras need to be installed on the water. That makes signal transmission problematic. The nature of ports involves many different groups of people with separate system infrastructures, and it is difficult to combine them all, leading to compatibility problems.

Another measure to increase the prevention efforts at seaports is the use of Non-Intrusive Inspection (NII) technologies to accelerate the screening of container traffic. Gamma ray and X-ray imaging systems are being used to screen conveyances for contraband, including weapons of mass destruction. Radiation Portal Monitors (RPM) provide a passive, nonintrusive means to screen trucks and other conveyances for the presence of nuclear and radiological materials. Density meters and fiber-optic scopes are being used to peer inside suspicious containers. Vehicle and Cargo Inspection System (VACIS) are also being used to examine dense freight in order to detect contraband, weapons, and other potentially dangerous goods.

Another promising practice in use at some ports is electronic tracking systems installed on trucks transporting containers in and out of the port. At any given time, port management is capable of determining the exact position of these vehicles and establishing their current operations. However, with many of these systems, protocols for their use are still in development, and the limits of these systems are still being uncovered. Also, ports that implement these type systems may have to overcome employee relations issues about the nature and purpose of these systems.

In *Boston* an “intelligent” video system has been installed around the port perimeter, with capabilities to analyze video content and provide alerts for suspicious behavior. This video system also applies to the waterside perimeter, and will have an automated alarm and tracking system. The Port of Boston has also used grant funds to install a backup power unit to operate lighting, cameras, access control and other security devices in case of a power outage. A Maritime Emergency Command Center has been created to monitor cameras installed throughout the Port of Boston, including the cruise terminal, cargo terminals, the Tobin Bridge, and other critical areas. The command center is equipped with intelligent video hardware and is alarm-driven. Also, optic equipment has been purchased to allow for conducting undercarriage inspections at the Port of Boston.

In *Charleston* several local law enforcement officers have been provided with portable radiation pagers. Project Seahawk has established an event-driven, intelligent monitoring system that incorporates radar, sensors, more than 100 cameras, thermal imagery, and radiation

dispersion detectors. Also, a computerized system to track cargo has been installed, allowing better information concerning the origins and contents of ships arriving at the Port of Charleston.

In *Galveston* the port obtained grant funds to purchase several CCTVs, but they are not yet "intelligent." As a result, an operator is needed to monitor the devices. In *Houston* the port authority has received grant funds to purchase and install more than 300 intelligent video systems, both on the land and on the waterways, visible from both the dispatch office and the command center. Cameras belonging to the Coast Guard and Texas are also available to the port police in Houston.

In *Jacksonville* dozens of intelligent CCTV cameras have been installed in several locations. Some are fixed and some have Pantel zoom capability. Sheriff's deputies can watch up to 16 cameras on laptops. In *New Orleans* CCTVs have been installed throughout the port, including dozens at the cruise ship terminal.

In *Savannah,* CCTVs (many of them intelligent) have been installed throughout the port, and a Security Control Center has been built to house monitoring facilities. Also the Port of Savannah purchased and operates its own Radiation Portal Monitors. Port police also have their own radiation isotope identifiers. In *Tacoma***,** CCTVs and detection equipment have also been installed throughout the port. Motion detection software was being installed at the time of evaluation site visit with Tacoma. The Port of Tacoma also uses a web-based Rail Management System. Using Geographic Information System (GIS) technology, this system provides on-line access to information concerning the location of rail shipments. This system has proved valuable in identifying the appropriateness of rail deliveries. Also, in *Texas City***,** CCTVs have been installed throughout the port and along the waterside.

Law Enforcement-Related Activities

Police patrol and related activities are another preventive measure being taken at seaports. While not new, police patrol at ports has increasingly involved partnerships among federal, state, and local law enforcement agencies, as well as private security firms and labor organizations. Seaport security varies considerably, depending upon the resources, statutory authority, and corporate policies of the individual seaport agencies. Many of the port police departments have increased the size of their agencies and patrol personnel, and some have switched to the use of certified/sworn personnel. One of the innovations we observed during our site visits was ports with their own 911 call centers for dispatching cases for the port police. And a number had, in addition to regular patrol units, special teams such as bike teams, dive teams, boat teams, bomb disposal units, crisis negotiation teams, criminal investigations units, and special response/tactical teams. We also learned that a number of ports are making use of K-9 units and report that canines can be very effective in checking containers for explosives, contraband (e.g., illicit drugs), stowaways and personnel entering the port. The use of canines at ports is a promising practice, for there are multiple purposes they can serve.

Depending on their size and needs, some ports have also developed entirely separate police agencies to handle certain functions such as securing port rail lines. Technology has also been a key aspect of patrol work at the ports we visited. On the waterside, we observed a variety of waterside perimeter protection systems (providing electronic surveillance around critical infrastructure and highly vulnerable vessels to provide early surveillance and auto threat detection and alarms), vessel tracking information systems with geographical interactive displays to provide capture and display information to monitor the exact location of vessels entering a waterway (especially in relation to critical infrastructure), and external interfaces for port

security to share data with other organizations such the U.S. Coast Guard and local law enforcement. On the landside, we observed a variety of access control systems; extensive use of wireless network communications; chemical, biological, radiological, and nuclear detection systems, and a variety of other smart camera surveillance systems to notify key personnel of security breaches. Below we discuss some of the internal changes we observed in port policing, efforts to improved collaboration among law enforcement agencies, and promising examples of inter-agency cooperation.

Internal agency changes. We observed a number of promising internal changes at the seaports we visited to facilitate terrorism prevention. Below are some examples of these changes.

In *Boston and Savannah,* additional port police officers have been hired, trained, and deployed since 9/11.

In *Charleston* the port has begun to inspect all luggage and stores for cruise ships, using explosive-detecting K-9s. Also, when handling cruise ships, overtime officers are used to supplement the police presence during embarkation. At railroad entries, port police officers must be present when a train enters the Port of Charleston. Cameras are also used to monitor the entry gates.

Next, the port police in Charleston have created a unit that is trained and equipped to remain on the port when everyone else is evacuated during a crucial incident. This resulted from the experience of the New Orleans Port Police, who were ordered to evacuate the port during Hurricane Katrina, leaving the port temporarily without law enforcement protection.

In *Galveston* the port police work closely with private security to ensure security of the cruise ship terminal when a ship is in port. Also, Sea Marshals ride at-risk ships in and out of the port. The Port of Galveston has also hired more port police officers since 9/11.

In *Houston* additional port police officers have been hired. A command center in which all CCTVs can be viewed and operated has been created at Houston port police headquarters. Also, a mobile command center vehicle that replicates many of the command capabilities of the port police has been purchased with grant funds. When a cruise ship is in the Port of Houston, all luggage is subjected to X-ray analysis, stores are sniffed by dogs for explosives, and special attention is paid to ensure that only qualified personnel are in the vicinity of the ship.

In *Jacksonville*, Florida's 2000 security legislation requires the full-time presence of law enforcement officers in the state's major ports. As a result, a memorandum of agreement was signed between the Jacksonville Sheriff's Office and the Jacksonville Port Authority in November, 2002 that contracted for 10 sheriff's deputies to provide law enforcement services on the port. Since that time, although the port has created its own department of security, the number of contracted deputies has significantly increased.

In *Long Beach***,** the Long Beach Police Department created a "boat detail" to provide law enforcement on the port. This unit works closely with the port's Harbor Patrol. Also, the Long Beach Police Department's Anti-Terrorist Division has a liaison officer stationed on the port to collect and disseminate intelligence concerning threats to the port.

In *Los Angeles,* the port police department has greatly increased its number of sworn port police officers. The port police have also increased community policing activities, in which officers inform the public about the importance of observing suspicious activity and informing the police about what they have seen. The Los Angeles Port Police have also developed a Dive Team to work with the Coast Guard to investigate spills, accidents, and suspicious incidents. The Los Angeles Port Police also contribute officers to the work of the the Sea Marshals, who

are also comprised of Coast Guard personnel. The marshals board cruise ships when they enter and exit the harbor, to increase security.

In *Miami*, upon the arrival or departure of a cruise ship, Metro-Dade Police officers conduct a thorough search of the cruise terminal and turn it over to private security during the boarding process. In accordance with Florida law, sworn officers maintain perimeter security. All provisions are scanned for explosives. Also, Metro-Dade officers have intensified their random patrols throughout the port, have added more check points, and have also intensified their attention to the entry gates and beneath the bridge leading to the port.

In *New Orleans* more port police officers have been hired, trained and deployed. Also**,** New Orleans Port Police officers have been provided with radiation detectors to wear on their belts. They are encouraged to use these on suspicious vehicles and persons.

In *Port Everglades* the Broward County Sheriff's Office created a Harbor Unit to focus on the port, and the number of officers assigned to this unit has been greatly increased. The Sheriff's Office has also created a Domestic Preparedness Unit and a Terrorism Unit, both of which are available to the port. Also available to Port Everglades is a "Trident Team" of divers from the Coast Guard, the Broward County Sheriff's Office, the Broward County Fire Department, the Fish and Wildlife Commission, and the Department of Homeland Security. The Trident Team has been created to inspect risk-prone ships and facilities.

In *San Diego* the Harbor Police have added more police personnel, created a Homeland Security unit, increased the number of their K9 explosive detection teams, and expanded the dive team and maritime patrol operations. Also in *Seattle,* the Washington State Police have instituted strict vehicle screening systems, using explosive-detecting K9s, to detect Improvised Explosive Devices (IEDs).

Improved collaboration among law enforcement agencies: We observed a number of promising examples of collaboration among law enforcement agencies at the seaports we visited. Below are some examples of these collaborative efforts.

In *Boston*, when a Liquefied Natural Gas (LNG) tanker enters the port, extensive collaboration by many agencies (Coast Guard, State Police, local police agencies, port police, and others) creates a protective zone around the tanker. The potential for a catastrophic disaster with LNG tankers is something of deep concern to port officials. Take-offs and landings are halted at Boston's Logan Airport as the LNG vessel passes alongside several of the airport runways. The tanker is surrounded by escort vessels alongside it and helicopters above. The Coast Guard's rules state that all other vessels must keep clear two miles ahead and one mile behind a moving LNG tanker, with no vessels moving at all alongside it in the narrow confines of the inner harbor. Dozens of federal, state, and local law and safety agencies, as well as the private sector, are involved in securing an LNG tanker approach to the Port of Boston.

The security measures described above are only examples of a very intensive set of protocols to create a "security bubble" around LNG tankers on the water, in the air, and on the ground. When a cruise ship is in port, port police, state police, and private security guards work together to sweep the terminal with explosive-sniffing dogs, provide security, and control traffic. The Massport Police and Massachusetts State Police work collaboratively to share responsibility for port security.

Galveston has created a multi-agency dive team to detect explosives on high-risk ships. In *Houston*, several local law enforcement agencies have signed memoranda of understanding (MOUs) affirming how they will come to each other's assistance in the case of an emergency.

In *Jacksonville* a memorandum of understanding (MOU) has been signed between the Jacksonville Port Authority and the Jacksonville Sheriff's Office. This MOU gives operational control of sheriff's deputies and private security guards to the port's Director of Security. Unlike some other sites that contract for law enforcement services, this ensures a unified chain of command. The Security Director is also involved in the selection of deputies to be assigned to the port. Another example of a collaborative effort at the Port of Jacksonville: When a cruise ship is in port, representatives of the Coast Guard, the Jacksonville Sheriff's Office, and private security work collaboratively to provide security. And during military outloads, military security, sheriff's deputies, and agents of Florida Fish and Wildlife work closely together to provide security.

The Port of *Los Angeles* has developed a program called Operation Archangel. Operated by the Los Angeles Police Department, the Los Angeles Sheriff's Department, fire departments, and 12 other local agencies (including the Los Angeles Port Police), the program aims to identify and protect critical assets in the metropolitan area. Its purpose is to defend likely targets against catastrophic terrorist attacks through a cooperative agreement with the Office for Domestic Preparedness, a core group of city, county, federal, and private organizations that are collaborating to prevent and protect against terrorist attack. The operation identifies and prioritizes critical assets; creates partnerships to protect those assets; compiles a Critical Asset Assessment for each asset, with information of use to incident commanders concerning important aspects of that asset; designs critical incident management systems to respond to incidents at that location; and produces training and exercises designed to best respond to threats.

In *New Orleans,* when a cruise ship is in port, officers from the port police, New Orleans Police Department, and private security work together to provide access control, traffic control, and perimeter control. The Port of New Orleans also has a Joint Operations Committee that is constituted anytime a critical incident occurs. Members include the FBI, CBP, the Coast Guard, the Department of Homeland Security, and ICE. If the incident is not maritime-related, the Coast Guard representative does not participate. In another collaborative effort, the Coast Guard and local law enforcement have a Memorandum of Understanding to provide local law enforcement with the authority to enforce maritime law.

In *San Diego* there is a Blue Force Tracking System to distinguish between law enforcement agency vessels and commercial and recreational vessels. In *Savannah,* when a ship carrying ammonia is in the Port of Savannah, several agencies work together to provide security. Similarly, when a cruise ship is in the Port of Savannah, the Coast Guard flies a helicopter over the cruise facilities; divers are sent underneath the berth to look for explosives; and law enforcement provides coverage. In *Seattle*, when a cruise ship is in the port, officers from several local police departments work with port police to provide security and manage traffic around the cruise terminal. Port police in Seattle inspect and verify stores at a site away from the cruise terminal; only stores that have a verification ticket are allowed near the cruise terminal. In addition, the Port of Seattle has purchased unmarked transmission X-ray machines that inspect vehicles in the cruise terminal area from a distance.

Inter-agency cooperation. We observed several promising examples of interagency cooperation at the seaports we visited. Below are some examples of these cooperative efforts.

In *Long Beach,* the Police Department has established a Harbor Unit that focuses on providing law enforcement and ensuring security at the Port of Long Beach. This unit works closely with non-commissioned security personnel of the port's security force.

In *Los Angeles,* the Port Dive Operations Group (PDOG), made up of certified divers from the Coast Guard, the FBI, the Los Angeles Port Police, the Los Angeles Fire Department, the Los Angeles Sheriff's Office, and the Long Beach Fire Department, is available to respond to critical incidents. In addition, the group meets quarterly to discuss training and operational issues. And the Sea Marshals Unit at the Port of Los Angeles (comprised of divers from the Coast Guard and the Los Angeles Port Police) conducts joint dive operations to protect ships in transit and inspect critical infrastructure.

The Port of *Texas City* purchased a patrol boat with Port Security grant funds. Since the port does not have a police force or a security department, port officials signed a MOU with the Galveston Sheriff's Office to use the new boat to patrol the premises of the port of Texas City.

In the Ports of *Seattle* and *Tacoma,* the port authorities have demonstrated high levels of inter-agency cooperation with the U.S. military. The Port of Seattle currently serves as a West Coast Army seaport. The region around the Port of Seattle is host to a contingent of Army, Navy, Air Force, Army Reserve and National Guard facilities. Nearby the Port of Tacoma also serves as a strategic military transport site for U.S. military operations and has been used to stage a variety of military and Homeland Security exercises over the years. Having a military operation connected to a seaport presents a special set of security concerns. The Coast Guard is responsible for security at the port, but the military is responsible for security on its vessels, and the lines of jurisdiction can become blurred. One side benefit of a port that serves as a military seaport is that port personnel grow accustomed to heightened security practices, as required by their ongoing participation in military shipments and exercises.

The Port of Seattle is also a partner in an international economic cooperative. The Port of Seattle joined a program of the Asia Pacific Economic Cooperation (APEC) known as Secure Trade in the APEC Region. The port was an integral partner in the Bangkok/Laem Chabang Efficient and Secure Trade project in 2003. The project demonstrated end-to-end supply chain security between Thailand and the United States.

At an APEC meeting, the U.S. Secretary of State presented a video produced by the Port of Seattle that gave an overview of the project as a model of security measures to be considered for broader application. For example, the Port of Seattle is the first port in the nation to enter into formal partnerships with the government of Thailand and the Ports of Singapore and Hong Kong to demonstrate container security practices. This new system will catalog and inspect U.S.-bound cargo at foreign ports. It will allow U.S. authorities to track the shipments through their entry into the United States and on to their final destination. For shippers, the STAR program provides a system to secure, track and manage the supply chain, which can reduce expenses by cutting logistics and inventory costs and increase revenue by improving service rates. For importers, the STAR program offers a secure system with the financial benefits of shorter transit times and reduced inventory safety stocks.

Interagency Operation Centers

Interagency operation centers can greatly aid jurisdictions in connecting the large volume of data on threats to a port, which is greatly outstripping the number of analysts available to explore the data. Based on our field work, we observed that collaboration across agencies can help improve the fusion of data from many disparate data sources to provide greater awareness and monitoring of threats to a port, coordination of incidents, and response activities. Various agencies, including the Department of Homeland Security (through the U.S. Coast Guard), the Department of the Navy, and the Department of Justice, have developed interagency operational

centers at certain port locations. These are centers where multiple federal (and in some cases, state and local) agencies are co-located in one facility and work together to monitor maritime security and planning-related operations. The evaluation team visited four of these centers.

In *Charleston* there is the Charleston Harbor Operation Center (CHOC), commonly known as Project SeaHawk. Seahawk is a coordinated multi-agency pilot effort, under the auspices of the U.S. Attorney, designed to create a unified law enforcement and intelligence operation. The goals are to deter and prevent acts of terrorism, manage a joint operations center to track maritime and other modes of transportation operations in the Port of Charleston, establish an interoperable system for intermodal data sharing and intelligence gathering, and provide a test bed for innovative concepts, initiatives, and equipment related to port security.

SeaHawk originally included 20 participating partner agencies, but by the time day-to-day operations started, that number had grown to 47. The agencies that joined SeaHawk brought different assets to the operation. While some brought personnel, others brought equipment and access to their databases. Seventeen federal, state, and local agencies have assigned full-time personnel to the operation. In addition, the FBI's Joint Terrorism Task force, the Coast Guard's Field Intelligence Support Team (FIST), and the port authority police department dispatch unit have co-located within the SeaHawk facility. More than two dozen other agencies participate on a part-time or "as needed" basis. Daily meetings of all members allocate resources to the most appropriate assignments. Some officers may conduct investigations; others might conduct gate checks or terminal checks, or use explosive-detection dogs to locate explosives. An intelligence unit combines intermodal transportation and harbor security data—including video camera feeds, radar, and thermal imaging—along with information about crews and cargo, to assess potential threats. A marine unit is involved with escorting vessels, providing security training, reaching out to community members, and boarding suspicious vessels. SeaHawk is also making use of the latest technology, such as an event-driven camera monitoring system that incorporates sensors, cameras, thermal imagery, and radiation dispersion detectors. Project Seahawk began with $9 million in funding from the Department of Justice, and was allocated $29.5 million in federal funding for port security in 2004. Of that money, $22 million is funding the continued development of Project Seahawk, including about $9 million to renovate and equip a command center and $4 million to test existing port equipment that screens cargo for radioactive materials and chemical and biological weapons. The remaining $7.5 million is helping equip the project with the latest computer hardware, software, and communications infrastructure. Current SeaHawk funding provides support until May 2008.

The *Port of Miami* and the *Port of Everglades* have been piloting Project Hawkeye. This project provides the Coast Guard with a system of cameras and sensors to identify and track vessels in harbor and coastal waters. From its command center in Miami, the Coast Guard monitors commercial vessels there and in nearby ports and ocean channels, as well as the activities of small recreation vessels that act suspiciously. Images from Hawkeye's radar sensors and long-range cameras (with night-vision and infrared capabilities) are viewed on displays at the command center. This information is combined with data from an automatic identification system (a system required for domestic and foreign vessels over a certain tonnage, identifying the ship's name, tonnage, course, speed, and location). This system can learn the normal port activities and identify deviations from normal, alerting the Coast Guard to anomalies. With this information, the Coast Guard can make better decisions about which vessels should be intercepted and inspected.

In *San Diego* port officials operate the San Diego Second Command Center-Joint (SCC-J), previously known as the San Diego Joint Harbor Operations Center (JHOC). SCC-J co-locates representatives of local, state and federal agencies and arms them with smart technology to close port security gaps and increase port level maritime domain awareness.[28] Representatives of the Coast Guard, the U.S. Navy, the San Diego Harbor Police, the San Diego Police Department, the FBI, the California Highway Patrol, and the Department of Homeland Security (ICE and CBP) are housed in a Coast Guard facility and operate in one command center under the overall leadership of the Coast Guard. The agencies share feeds from intelligent CCTVs, radar, sonar, and other detection sensors. In addition, the agencies share access to information provided by all participating agencies, allowing the participants to coordinate planning and response to critical incidents and to complement each agency's capabilities.

In Virginia, a Joint Harbor Operations Center (JHOC) involves representatives of the U.S. Coast Guard and the U.S. Navy co-locating in one Coast Guard facility, sharing intelligence information, and coordinating operations. The center operates a system similar to those in Miami and San Diego, described above. The primary focus is on security information related to force protection for the Navy. Inside the center, homeland security personnel capture radar and sonar signals, track video and vehicle tracking data, take phone calls from the field, listen to radio traffic from patrols and commercial ships at sea, and break down classified intelligence information--all in an effort to prevent a terrorist strike or assist in maritime rescues. Using dozens of video and computer screens, about 50 Coast Guard and Navy personnel maintain a 24-hour watch on the waterways, bridges, tunnels and ports in Hampton Roads.

Preparedness

According to the National Incident Management System (NIMS), preparedness includes a range of tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from critical incidents. This includes establishing guidelines, protocols and standards for planning, training and exercises; improving personnel qualifications and certification; and certifying equipment.

The port security officials we talked with during our site visits all seemed to agree that to address the risk of a terrorist attack against a U.S. seaport, they need to increase their level of preparedness. Preparedness requires measurable demonstrated capacity to respond to acute threats with well-planned, well-coordinated, and effective efforts by all of the essential participants, including elected officials, police, fire, medical, public health, emergency managers, intelligence, community organizations, the media, and the public at large (see RAND report at www.globalsecurity.org/security/ library/report/2003/volume_v_report_only.pdf). Such preparedness requires sustainable, effective, and well-coordinated preventative efforts by the components of the intelligence community, law enforcement entities, and a well-educated and informed public (see RAND report at www.globalsecurity.org/security/ library/report/2003/volume_v_report_only.pdf).

In preparing for a terrorist or other physical attack on a port, it must be recognized that this is a very difficult task; any part of the port has the potential to be breached or destroyed. However, the thinking is that the more secure the port is and the better it is designed to withstand an attack, the greater the odds are that it will not be attacked, or if it is attacked, it will suffer less damage. Some of the ports we visited evaluate the terrorist threats against them and analyze for

[28] The center also supports the Coast Guard's missions beyond port security, including drug interdiction, alien migrant interdiction, and search and rescue activities.

factors such as the existence of the terrorist threat and groups hostile to the port, the capabilities of the terrorists, history of past terrorist attacks, the intentions of the terrorists and what they hope to achieve, and whether the terrorists are engaging in targeting activities such as surveillance. Terrorists attacks are rare events and few emergency responders are going to have direct experience handling such incidents. In this section we discuss a number of promising practices ports have taken to prepare for these types of rare events through training; field exercises; and models, simulations, and games.

Training

The Maritime Transportation Security Act (MTSA) requires that all ports provide periodic training and exercises. To address this issue, some ports have taken an approach that it is the responsibility of all port personnel to ensure the safety and security of themselves and others. The reasoning is that the greater the number of employees who are aware of what a potential threat may look like, the greater the likelihood of preventing an attack on the port. Providing "awareness training" to all port personnel on security issues allows for more people to notice something that is out of place. This is a fairly low-cost best practice.

In addition to this general type of training, some of the ports we visited had fairly extensive training programs (see below). An important and sometimes underemphasized part of port policing is the need to practice and train at a firearms range. To maintain firearms proficiency and accuracy, police and security officers should practice with their weapons as frequently as possible. Due to logistics and cost constraints, it is common for port police and security officers not to practice or qualify with their firearms as often as is desirable. To make firearms practice more accessible and inexpensive for officers, and to maintain and improve marksmanship qualifications, some port facilities are installing outdoor firing ranges complete with movable targets. Officers can practice with their firearms while they are on the facility at no cost, thereby remaining available to respond to a security incident. Depending on the size of the security force, the numbers of weapons they are required to maintain proficiency on, and the size and configuration of a facility, the installation of a shooting range on a facility can prove to be a good option for port police and security officers to maintain and improve their firearms skills. Below are other examples of promising practices we observed in the area of local training in port security issues.

Charleston. Earlier we described the Port of Charleston's Project Seahawk. An added advantage of having Project Seahawk in Charleston is the availability of facilities for training. Charleston is home to the Border Patrol Academy, which is being converted into a federal law enforcement training center. About 2,000 Border Patrol agents graduate each year from this academy. The U.S. Coast Guard has recently announced plans to move its maritime law enforcement school to the old Charleston Naval Base. About 2,000 Coast Guard trainees a year will pass through this new law enforcement academy. With the addition of this new Coast Guard academy, Charleston will continue to enhance its role as a premier location for port and maritime security. MTSA training also is provided on the Port of Charleston's website for use by all stakeholders.

Houston. At the Port of Houston, training has been provided to all employees concerning MTSA requirements. In addition, three-day training has been provided to private security guards, and Terminal Security Officers have received training.

Jacksonville. The Jacksonville Port Authority pays for members of the Jacksonville Sheriff's Office to attend a 40-hour seaport security class at the Federal Law Enforcement Training Center in Glynco, Georgia.

Los Angeles. Port Police in Los Angeles have established a security awareness training program, aimed at educating port employees and community members about signs of potential terrorist threats and how to report them.

Field Exercises

To assess coordination and response procedures that would be implemented in the event of a terrorist attack, officials in U.S. ports have conducted exercises that simulate a potential threat, attack, or incident. The MTSA requires that all ports engage in periodic exercises (tabletop and field) and simulations. Many of these exercises involve multiple agencies, designed to improve their ability to respond collaboratively to critical incidents. These exercises have addressed such scenarios as the explosion of a "dirty bomb" that releases radioactive materials, threats of an approaching ship that may have a bomb or other hazardous material aboard, and disruptive attacks on critical infrastructure or specific facilities within a port.

The United States Coast Guard has primary responsibility for port security, and conducts dozens of seaport-based terrorism exercises per year. These exercises vary in size and scope and are designed to test specific aspects of the Coast Guard's terrorism response plans, such as communicating with state and local responders, raising maritime security levels, or responding to incidents within the port. The training and field exercises are very complex and can involve dozens of federal, state, and local agencies including law enforcement, fire and emergency management, and a variety of other first responders. Exercises may also require close coordination across many jurisdictions, raising issues about how agency personnel can communicate effectively when they have different chains of command, communication systems, operating procedures, and equipment.

After these exercises are conducted, the Coast Guard requires that the unit participating in the exercise submit an "after-action" report describing the results and highlighting any lessons learned. Analysis of these reports presents an opportunity to identify potential barriers to an effective response during an actual threat or incident. These reports can also provide valuable input for future exercises conducted by the Coast Guard or other agencies.

A number of the sites we visited also are involved in the National Exercise Program (NEP) to increase preparedness. Homeland Security Presidential Directive (HSPD) 8 outlines actions to strengthen and measure homeland security preparedness, and cites the National Exercise Program as a priority initiative. The NEP establishes the framework for the scheduling, design and evaluation of exercises designed to test the response capabilities of the federal government and its state, local and tribal partners. Efforts are made to include international and/or private-sector participation.

The cornerstone of the national performance-based exercise program is the Top Officials (TOPOFF) National Exercise Series, a biennial program that includes a functional exercise in year one and a full-scale exercise in year two, with continuity provided by a series of seminars. In addition to full-scale, integrated, national-level exercises, the NEP provides for tailored exercise activities that serve as DHS's primary vehicle for training national leaders and staff. The ports we visited have found the NEP useful in increasing the collaboration among port partners at all levels of government, and providing a means to conduct "full-scale, full-system" tests of

collective preparedness, interoperability, and collaboration across all levels of government and the private sector.

Savannah. The Port of Savannah holds annual exercises and drills, including one-day multi-layered training exercises designed to refine, rehearse and validate homeland security plans. As part of the practice scenario, an alleged radiological dirty bomb is delivered in a container to the Port of Savannah. Testing their skills and capabilities, the responding agencies work out communication matrices to share information efficiently and accurately. These exercises bring together members of the Georgia National Guard's 4th Civil Support Team, the Bureau of Customs and Border Patrol, the Georgia State Patrol, the Chatham Emergency Management Agency, the Chatham County Emergency Management Agency, the Georgia Bureau of Investigation, the Coast Guard, Chatham County Explosive Ordnance Disposal, GPA Police, and a number of other federal, state and local first responders. This exercise helps the various responding agencies to identify areas of responsibility and coordination.

Jacksonville. The Port of Jacksonville uses computer simulation exercises of a terrorist bombing of a major commercial bulk and container terminal to assess the seaport's emergency response and evacuation plan.

Models, Simulations, and Games (MS&G)

Ports are increasingly using MS&G to better prepare first responders to respond to an attack against seaports. Ports are beginning to incorporate MS&G into training and exercises, and MS&G are becoming preferred planning and teaching tools. MS&G allow local officials to inexpensively plan for low-frequency, high-impact events. MS&G fits the ports' budgets and, ideally, can disseminate information learned in large exercises to smaller entities. Some of the ports we visited have been working with games that simulate reactions to biological and radiological events, strategic incident commander games, games that focus on the coordination problems associated with mass casualty medical triage, and even simulated human bodies on which to practice medical treatment. The prices range from nothing, for certain CD–ROMs, to $200,000 training simulators.

MS&G allow participants to respond as a team in real time to simulated emergency scenarios lasting two to eight hours, such as explosions or the release of radioactive contaminants or biological agents. The system tracks players' responses and provides real-time assessments of their expected actions, which permits each jurisdiction to determine strengths and areas of concern in advance of a real emergency. MS&G can approximate real conditions and improve training via: engagement of the senses (e.g., live voice communication); psychological and physical fidelity; realistic environments (e.g., weather, terrain); portrayal of perpetrators (e.g., actions taken and equipment utilized); situational conditions and events (e.g., gas plume area and dynamic spreading); resources and actions (e.g., fire apparatus, responder teams and decisions); situation parameters (e.g., resource arrival time, disposition of resources at the scene, tracking of resources to prevent duplicate use, etc.); experiential learning (i.e., learning through experience); awareness training of the lethality of weapons of mass destruction (WMD); and real-time unfolding of events in the aftermath of a WMD attack.

MS&G allow personnel to "experience" dangerous events without exposing them or the environment to actual hazards, without consuming actual resources (e.g., personal protective equipment kits) and with little or no possibility of accidental injury to participants. MS&G can reduce the limitations of real-world constraints (e.g., infectious disease training need not await a real outbreak, because such events involving myriad ailments can be modeled and medical

interventions "practiced" on simulated patients). MS&G also can provide the necessary experience to enhance the decision-making process in high-stress situations even as it allows participants in many cases to participate in simulations from their offices without requiring travel to common physical sites.

MS&G can also provide a means of evaluating plans by modeling consequences based on specific city conditions and resources (e.g., performing cost estimates of response and recovery). MS&G can also allow for exercises involving long-term impacts. Time inevitably is a critical factor in response and recovery efforts. To date, however, little attention has been given to the compounding effects of a WMD event on the "system of systems." In fact, for the most part only "direct effects" are modeled and trained. Secondary (e.g., multi-day) effects on transportation systems, wastewater treatment and waste disposal, recovery logistics systems, evacuation/victim management, etc., have been inadequately incorporated into curriculum design due to time constraints, modeling complexity, and lack of prioritization.

Response

Response, according to the National Incident Management System, includes activities that address the short-term, direct effects of an incident. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into the nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity and apprehending actual perpetrators and bringing them to justice.

A terrorist attack or similarly disruptive incident of national significance involving the marine transportation system can also have a severe ripple effect on other modes of transportation, as well as have adverse economic or national security effects. Responding to such incidents at a U.S. seaport might require immediate actions to save lives, protect property, meet basic human needs, and execute emergency operations plans. As we learned on our site visits, responding may involve the need to detect and rapidly identify WMD agents; react without endangering first responders; treat the injured; contain and minimize damage; rapidly reconstitute operations; and mitigate long-term hazards through effective decontamination measures. These actions could preserve life, property, the environment, and social, economic, and political structures, as well as restore order and essential services for those who live and work within the maritime domain.

The experts we consulted stressed the need, at the onset of a maritime incident, for Federal, State, local, and tribal authorities to assess the human and economic consequences in affected areas rapidly, and to calculate the effects that may radiate outward to affect other regional, national, or global interests. These entities must also develop and implement contingency procedures to ensure continuity of operations, essential public services, and the resumption or redirection of maritime commercial activities, including the prioritized movement of cargoes to mitigate the larger economic, social, and national security effects of the incident.

Although the National Response Plan and MTSA call for an attack on a port to be managed at the lowest possible organizational and jurisdictional level, maritime incidents of national significance will require the federal government working with state and local governments and the private sector. Similarly, there is a need for corresponding international coordinating mechanisms to reconstitute commerce and minimize the global impact in the event

of a significant maritime incident or threat. Therefore, much of what we observed during our site visits in the area of response practices were more generic promising practices as they relate to the application of federal guidelines from the National Response Plan and MTSA. However, in some cases there have been some unique jurisdiction-specific response practices established, and these areas will be highlighted and discussed.

Responding to an attack against a port requires planning for uncertainty, fast action in moments of crisis, and operations that almost always cross external and internal agency lines (see Haveman and Shatz, 2006). Many of the ports we visited used the Incident Command System to deal with these issues during multi-agency and multi-jurisdiction emergency response. The Incident Command System has many attractive features and is something that other ports should consider adopting.

Under the Incident Command System, the agency overseeing emergency operations depends on the nature and location of the event. During a multi-jurisdictional event, agencies establish a "Unified Command" where agency managers share decision-making responsibility within a group. There is no formal leader. Individual agencies maintain operational control and responsibility for their own assets and personnel, and agency leaders are supposed to act cooperatively, transferring decision-making authority within the Unified Command group, based on changes in the nature of an incident. This system allows agencies to adapt to changing situations by avoiding a rigid organizational structure. However, its effectiveness hinges on informal trust, cooperation, and institutional knowledge about which agency leads under what circumstances (see Haveman and Shatz, 2006) — issues that can be worked on through regular training and exercises. In this section we discuss two main areas that could be considered promising practices in responding to an attack against a seaport: Exercise and Training; and various Team Responses.

Exercise and Training

Exercises and training programs are among the key activities that a seaport can undertake to prepare to respond to a terrorist attack. Under this heading, we identified a number of promising practices, including Seattle's Marine Terrorism Response (MTR) Project, the Maritime Incident Resources Training Partnership (MIRT) in Boston, and local participation in the DHS-developed Port Security Exercise Training Program (PortSTEP).

Seattle's Marine Terrorism Response (MTR) project: With DHS/Office for Domestic Preparedness (ODP) funding, the Port of Seattle was awarded $2 million to operate a national seaport security exercise and training pilot program for emergency responders. MTR represents one of the most extensive exercise and training programs developed for the maritime environment. The objectives of the Marine Terrorism Response (MTR) Project are to: minimize the impact of marine terrorism on life, property and the environment; achieve an improved, sustainable maritime terrorism response capability that is also applicable to other marine emergencies; engage local and national agencies and maritime community representatives in the development of a regional and national Marine Terrorism Response Plan; support the implementation of Homeland Security Presidential Directive (HSPD) 5 (Coordination) and HSPD 8 (Preparedness); and ensure the Plan complies with the NRP (National Response Plan) and NIMS (National Incident Management System).

The MTR plan includes three volumes of materials: Volume 1 is a preparedness plan, Volume 2 is a response plan for handling an attack against a port, and Volume 3 is a field operations guide for emergency responders. The MTR plan meets Office for Domestic

Preparedness (ODP) guidelines and includes: web-based training, classroom/vessel training, and field exercises. Web-based training provides continuity of material delivery. All students can access the same material, and can access classes 24/7. The training is adaptable to local jurisdictions and validated by on-line testing, and a certification of completion can be downloaded by students. Classroom/vessel training involves 16 hours of programming designed for incident commanders, providing unified command training on vessel familiarity, vessel damage stability, integration of shore-based command with marine incident response agencies, and lectures by local Coast Guard response teams.

Three types of exercises are conducted: (1) tabletop exercises, (2) functional exercises (eight hours covering four scenarios), and (3) a full-scale exercise (two days covering four scenarios, involving 27 agencies and 647 participants, 185 victims and 90 controllers/evaluators). These exercises provide benefit to all the regional response partners through planning and conducting of a realistic set of exercise scenarios; demonstrating command, control, coordination, and communication between private and public response agencies and assets; demonstrating horizontal and vertical coordination between local, regional, state, and federal agencies; and demonstrating implementation of NIMS and the Incident Command System in a multi-agency, multi-jurisdiction exercise.

MTR involves several local public agencies (emergency management, law enforcement, fire service, and EMS providers), county public agencies (county emergency management and public health), regional partners (State Homeland Security Regions; Ports in Everett, Seattle, and Tacoma; and the Puget Sound Marine Firefighting Commission), state government partners (state emergency management, Department of Transportation, and Department of Ecology), federal government partners (DHS/OG&T, U.S. Coast Guard, FBI, EPA, Department of Defense, FEMA, CDC, Department of State, CBP, ICE, MARAD, and NOAA), international partners (Transport Canada), and private-sector partners (Washington State Hospital Association, cruise vessels, private ambulances and EMS, Washington State Maritime Cooperative, and Marine Response Alliance).

Maritime Incident Resources Training Partnership (MIRT) at the Port of Boston. The MIRT is an initiative started by local fire departments. Participants include the Massachusetts Port Authority (Massport), the United States Coast Guard Marine Safety Office in Boston, the Massachusetts Emergency Management Agency (MEMA), and the Massachusetts Fire Academy as well as numerous coastal communities concerned with maritime safety issues (Boston, Massport, Everett, Chelsea, Revere, Braintree, Clinton, and others). The main goal of MIRT is to provide training to local fire departments and support agencies that are called upon to respond to shipboard fires as well as other maritime emergencies that could occur in Massachusetts waters. MIRT was formed to help train local Massachusetts fire departments in emergency maritime incident procedures. An emergency maritime incident is one that would require the involvement of several agencies in a shipboard or waterfront incident and would normally overwhelm an individual agency's capabilities. Another goal of MIRT members is to expand current response capabilities and enhance maritime safety through regular training and field exercises using a unified command system. MIRT activities include drills on firefighting systems and tabletop exercises regarding shipboard fires and biological weapons on a cruise ship.

The Port Security Exercise Training Program (PortSTEP). The Transportation Security Administration (TSA), in partnership with the U.S. Coast Guard (USCG), has developed the Port Security Exercise Training Program (PortSTEP) as a joint program to help meet the mandates of

the 2002 Maritime Transportation Security Act (MTSA). TSA, being concerned with the surface transportation system, focuses on the intermodal aspects of PortSTEP, while the Coast Guard focuses on the water-side and maritime aspects of the program. PortSTEP was established to develop port security exercise and evaluation services and solutions for maritime and surface industry partners under the guidance and direction of the U.S. Coast Guard. PortSTEP brings together government and private-sector officials responsible for maritime transportation and commerce, emergency response and land transit in 40 port districts around the United States. Officials participate in fictitious incident scenarios intended to reflect the terrorist threat environment.

A number of our research sites have been involved in PortSTEP and consider it a promising practice in that it provides port security training exercises through the Area Maritime Security (AMS) Committees to include a mix of basic tabletop, advanced tabletop and functional exercises. PortSTEP is designed to achieve several performance objectives aimed at improving the intermodal transportation industry's ability to prepare for and contend with a transportation security incident. These objectives are centered on increasing stakeholder awareness and involvement through an outreach program; encouraging stakeholder participation in program development; encouraging program alignment with national standards and requirements; improving processes, creating partnerships, and delivering port incident training through the exercise program; and refining the program through evaluation and continuous improvement. PortSTEP has tailored specific exercises and objectives, developed measurement criteria, leveraged lessons learned from other security programs, and developed a set of innovative mechanisms for stakeholders to promote exercise participation and involvement.

The 40 sets of exercises are being conducted in seaports and inland ports of various sizes and terrorist threat profiles, ranging from Chicago to San Juan, Puerto Rico. The first PortSTEP exercise occurred in San Francisco in August 2005. Seven more occurred in 2005 in Baltimore; Anchorage; Boston; Puget Sound, Washington; Corpus Christi, Texas; Tampa, Florida; and Duluth, Minnesota. Exercises are being customized to the ports' varying situations, potentially involving threats to cruise ships in San Juan or to sea commerce in Long Beach, Calif. Scenarios range from how officials react to discovering a suspect cargo container, to an explosion at a seaport rail yard. Exercises follow the basic Homeland Security Exercise and Evaluation Program (HSEEP) methodology. A series of planning meetings take place in advance of the exercise that identifies exercise objectives, scope and requirements. Upon completion of the exercise, a robust evaluation and after-action report (AAR) is written that includes a plan of action to systematically correct deficiencies identified during the exercise. The AAR serves as the tool for communicating to the port community recommended actions to strengthen port readiness, and is provided to the local port committees for implementation.

Each PortSTEP exercise builds on the experience previously gained in a continual effort to deliver a top-quality product and maximize its value in enhancing security of ports and intermodal systems. A total of 17 exercises were scheduled for 2006, building toward the objective of conducting 40 exercises. PortSTEP development should be completed by the end of 2007, culminating in a fully vetted and tested port and transportation security exercise pilot program that can serve as a model for TSA and other government agencies.

Team Responses

Nearly all the experts we talked with on our site visits pointed to the need for strong partnerships in responding to a terrorism incident at a seaport. A number of the more promising efforts are reviewed below.

Boston--Maritime Incident Resources Training Partnership. Based on Norfolk's Maritime Incident Response Team, this initiative was started by local fire department officials, who were concerned that land-based firefighting was not appropriate for fighting fires on board ships. Participants include the Massachusetts Port authority, the United States Coast Guard Marine Safety Office, the Massachusetts Emergency Management Agency, the Massachusetts Fire Academy as well as numerous local communities that are concerned with maritime safety issues. The main goal is to provide training to local fire departments and support agencies that are called upon to respond to shipboard fires as well as other maritime emergencies.

Charleston--The Port Emergency Information Center. This center collates and distributes information to port stakeholders about the status of emergencies and what is required to reopen the shipping channel.

Charleston--The Port Operations Emergency Center. This center works with affected agencies, including the Coast Guard, the National Guard, and others to coordinate responses to emergencies.

Charleston--The Marine Fire Fighting Protocol. This is a grant-funded protocol used to train firefighters in the area on how to fight fires on the waterfront.

Houston--The Channel Industries Mutual Aid (CIMA). CIMA is a nonprofit organization combining the firefighting, rescue, hazardous material handling, and emergency medical capabilities of the refining and petrochemical industry in the Houston Ship Channel area. Formed in 1955, this organization provides cooperative assistance and expertise for all kinds of emergencies—both natural and man-made. CIMA members—who include industrial companies, municipalities, and government agencies—work cooperatively in four geographic zones. Groups in these zones maintain a corps of highly trained emergency personnel and a pool of more than 200 pieces of equipment, including rescue trucks, high-volume foam pumpers, and fully equipped ambulances. Joint operations are controlled from sophisticated command vehicles that link CIMA members via a common radio system. Response personnel are trained in both classroom and simulated emergency situations. Frequent refresher drills help maintain their response skills.

Houston--Division of Ship Channel. The Houston Ship Channel has been divided into nine areas, so that damage can be assessed separately and recovery plans can be coordinated.

Houston--Automated telephone and e-mail system. The Area Maritime Security Committee has instituted an automated telephone and e-mail system to alert all members and port stakeholders of information concerning security issues.

Los Angeles--The Community Emergency Response Team (CERT). CERT is a group of civilians organized as a neighborhood-based team that receives special training to increase their ability to recognize, respond to, and recover from major emergency or disaster situations. Teams are trained by professional responders in areas that will help them take care of themselves and others before, during and after a major emergency. As an organized team, individuals can

provide vital services while waiting for the arrival of emergency responders, and can assist once responders arrive. The CERT concept was developed and implemented by the Los Angeles City Fire Department in 1985 as a way to train civilians to function both as members of a CERT team and as individual leaders who would direct untrained volunteers during the initial phases of an emergency. The Federal Emergency Management Agency (FEMA) adopted the Los Angeles CERT model, and since the September 11 attacks has been directing grants to fund civilian CERT programs in all 50 states.

The CERT Program educates people about disaster preparedness for hazards that may impact their area and trains them in basic disaster response skills (see www.citizencorps.gov/cert/faq.shtm). Training typically covers areas such as disaster preparedness, disaster fire suppression and hazardous materials, disaster medical operations, light search and rescue, damage assessment, disaster psychology, debris management, homeland security, and team organization. Using the training learned in the classroom and during exercises, CERT members can assist others in their neighborhood or workplace following an event when professional responders are not immediately available to help (see www.citizencorps.gov/cert/faq.shtm).

Los Angeles--The Port Joint Operations Center. This center has members from the Port of Los Angeles Police, the Los Angeles Sheriff's Department, the Los Angeles Police Department, the California Highway Patrol, the U.S. Coast Guard, and CBP. The Center goes into operation when the threat level at the port goes to the orange level. The members collect intelligence information, assign and manage resources, and direct responses to terrorist attacks.

Los Angeles--Archangel. This is a DHS-funded project by the Los Angeles Sheriff's Department, the Los Angeles Fire Department, and the Los Angeles Police Department that compiled a catalog of potential high-threat locations and makes information available to first responders so that they can react to a terrorist attack with knowledge of the conditions they will face.

Savannah--The Marine Spill Response Corporation (MSRC). MSRC is a nonprofit, national spill response company dedicated to rapid response. MSRC was created in 1990 to respond to oil spills, shoreline cleanup, and hazardous material spills. The Port of Savannah has signed an agreement that MSRC will respond to any spill on port property.

Texas City--Port alert system. This system has been created to notify all tenants and port stakeholders of any critical incident.

Virginia--Maritime Incident Resources Training (MIRT) partnership. MIRT is a partnership that has created a team of fire fighters who have experience in fighting shipboard fires and have purchased equipment that can be used in extinguishing such fires. MIRT has also developed a training curriculum that has been used to train hundreds of firefighters and other professionals from the Norfolk area as well as from all over the United States. Other jurisdictions, such as Boston, have adopted this approach.

Recovery

As defined in the National Incident Management System (NIMS) plan, recovery involves the development, coordination, and execution of service/site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental and public-

assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents.

Recovery is an important issue, as billions of dollars worth of cargo pass through the U.S. port system on a daily basis. If the port system is closed in response to a significant incident, ports need to have protocols and be ready to implement them to efficiently resume port operations. Delays in reopening port facilities could result in dramatic, long-term economic consequences on a national scale (see Haveman and Shatz, 2006).

While many port security experts point to the near-inevitability of a terrorist attack against a U.S. seaport, little work has been done in the area of recovery from such an attack. Most of the work, as described earlier, focuses on improving marine domain awareness, prevention, preparation and responding to an attack, with little attention to how ports would get back up and running after an attack. In the Public Policy Institute of California's recent study, Haveman and Shatz (2006) argue that because there is no foolproof way to protect America's ports from a terrorist attack, the current focus of policies and programs should be directed much more toward comprehensive recovery plans to reduce economic panic and to restore global supply chains quickly following a catastrophe. Haveman and Shatz argue that how well the government reacts to the problems caused by an attack is probably as important as how well it anticipates them. In fact, the authors suggest that rigorous recovery plans can serve as a disincentive to terrorists, who have been shown to focus on targets where they can do the most damage—economic and otherwise.

One of the key areas covered during our visits, in this area of recovery, was the need to assure continuity of port operations to maintain vital commerce, with a focus on expediting the recovery of maritime infrastructure, transportation systems, and affected maritime communities. While certainly not a consensus view, some of the experts we talked with believed that the response to an attack does not necessarily mean an automatic shutdown of the marine transportation system. These experts would prefer a measured response based on an assessment of the specific incident, including available intelligence. These experts pointed out that certain operations may be continued by disengaging selectively only designated portions of the port, and immediately implementing contingency measures to ensure the public's safety and continuity of commerce. Accurate assessments regarding closures of selected nodes within the marine transportation system, as well as effective efforts to redirect the affected modes of commerce, can only be achieved with the full cooperation of the private sector.[29] This approach is consistent with DHS's recommendations for effective recovery, including[30]: (1) a common framework with clearly defined roles for those charged with recovery; (2) ready forces that are properly trained and equipped to manage incidents, especially those involving WMD; (3) carefully crafted and exercised contingency plans for response, assessment, and recovery; and (4) extensive coordination among public, private, and international communities.

Compared to the other four areas already discussed, on our site visits we did not observe or learn about very many promising practices in the area of recovery. This is unfortunate, for actions such as these steps could go a long way in preserving life, property, the environment, and social, economic, and political structures, as well as in restoring order and essential services for

[29] See http://www.whitehouse.gov/homeland/maritime-security.html.
[30]See http://www.whitehouse.gov/homeland/maritime-security.html.

those who live and work within the maritime domain. Nevertheless, we did talk with local port officials about promising practices in establishing recovery implementation plans and using a consequence management approach to recovery.

Recovery Plans

We observed a number of promising examples of recovery planning in Houston, Los Angeles and Seattle.

Galveston/Houston--Port Coordination Centers (PCC). The Captain of the Port (COTP) in the Houston/Galveston area has established four Port Coordination Centers in the ports of Houston, Galveston, Freeport, and Texas City to inform and advise the COTP concerning port operational and infrastructure needs, including security concerns that arise in the case of an emergency. Members of the Centers represent the ports as well as pilots, refiners, terminals, tug operators and other port stakeholders. The Centers can convene functionally in the case of a natural disaster, or geographically, in the case of a security incident. Each PCC designates a liaison officer to the regional Port Coordination Team (PCT) in order to establish shipping priorities, manage the flow of vessel movements, preserve safety and security, and implement established emergency protocols. The PCT's role is to disseminate information concerning the nature of the threat, implement protective strategies, continue communication to update the strategies, and reopen the port in an orderly manner. Also, at the Port of Houston, a subcommittee of the Area Maritime Security Committee (AMSC) has been created to develop protocols concerning how to shut down and bring back on line the port if it is shut down because of an emergency.

Seattle--Business continuity plan. In Seattle the port authority has developed a business continuity plan that spells out how to decide which operations go back in business in which order.

Los Angeles--Business resumption plan. At the Port of Los Angeles, the port authority has produced a business resumption plan to direct reopening of port after it has been closed due to a terrorist attack.

Consequence Management

Consequence management involves a formal process for the cleanup and restoration function after a catastrophe (e.g., an act of terrorism). Consequence management addresses the ways and means to alleviate the short- and long-term physical, socio-economic, and psychological effects of a catastrophe (see Seiple, 1997). In the context of an attack against a port, it includes the coordination of international, national, regional, and local assets to deal with the effects of such an attack. The term includes preparatory work in response to a threat, including site surveys; assessment of the ability of local hospitals to treat or decontaminate victims; and the size, condition, and locations of local stocks of various antidotes (see Seiple, 1997 at www.carlisle.army.mil/usawc/Parameters/97autumn/seiple.htm). Preparation could include determining the locations, size, and availability of other national antidote stocks as well as international stocks available to support planning for surge capacity (see Seiple, 1997). Consequence management would include treatment of victims within a contaminated zone, their decontamination and evacuation, and local cleanup. It would also involve psychological treatment and other efforts to restore confidence in the social and economic well-being of the affected area(s).

Consequence management could be a very helpful approach for seaport officials to consider adopting. In Chris Seiple's (1997) article on consequence management,[31] a number of his recommendations are relevant for seaports to consider in adopting a consequence management model, including: needing to establish coordination mechanisms to oversee the entire immediate response before federal assets arrive; planning for the use of federal assets to augment the existing response structure; examining the role of the military's reserves in a tiered response between the first responders and the arrival of federal help; planning for surge capacities that will be needed for different types of response; developing plans for tactical coordination at the incident site; developing model and specific evacuation plans; planning for who will handle the information campaign; planning for the role of medical facilities; and ensuring that fire and police departments are prepared to work together.

While responsibility for consequence management of WMD and other major attacks rests with the Federal Emergency Management Agency (FEMA), local ports need to be aware of the various elements of consequence management, receive training on it, and exercise using it. Based on our discussion with various ports officials, a number of recommendations emerged in the area of consequence management. First, ports should consider adopting a consequence management awareness/training program and a certification process for all levels of response to avoid disparate approaches that could inhibit communication and coordination. Second, identify, train, and mentor individuals within organizations on consequence management. Like many new problems that demand new partners, a new culture must be created to deal with the consequences of terrorism. Without "growing" such a culture, organizations will not be able to respond effectively and efficiently to either crisis response or consequence management tasks. Third, develop a tiered continuum of response. All national assets, such as the Chemical-Biological Incident Response Force, unless already deployed to potential terrorist targets, are generally not going to be able to respond to an incident within 6 to 12 hours. In that case, local responders will have to carry the burden of the immediate response.

While not a specific site in our study, we are aware that the Port Authority of New York and New Jersey has done consequence management training for its seaport personnel and stakeholders through a DHS sponsored "war game." In the exercise, there is a simulated massive disruption which causes a complete shutdown of the New York/New Jersey port. The exercise includes working through problems such as when the port would reopen again and what cargo would get priority. For example, do oil and chemicals move first, or food and retail? And how are passengers to be handled? The exercise participants also have to consider the long- and short-term economic impact of a complete shutdown. This is one of the few exercises we are aware of that is geared towards consequence management and business resumption. Consequence management is an important capability needed by seaports, and other seaports should consider completing exercises similar to the one just described.

Below are examples of ports we visited that were using or working towards a consequence management approach.

Houston--Portwide Security Council. This council is composed of approximately 70 companies working together to secure grant funding for buffer zone and security zone issues and to make plans for consequence management.

Houston--Port Strategic Security Council Steering Committee. The purpose of this council is to identify, seek funding for, and implement strategic security projects within the

[31] Seiple, C (1997). Domestic Response to Weapons of Mass Destruction. *Parameters,* Autumn 1997: 119-34.

jurisdiction of the area's Captain of the Port. This council consists of 11 voting members and is comprised of representatives from agencies regulated by the MTSA, Harris County, the Port of Houston Authority, the East Harris County Manufacturers Association (EHCMA), Channel Industries Mutual Aid (CIMA), Maritime Community representatives appointed by the West Gulf Maritime Association and the Greater Houston Port Bureau, the City of Houston, and cities of East Harris County. Non-voting representatives of the Steering Committee come from the Coast Guard, CBP, ICE, the U.S. Attorney, the director of Harris County Homeland Security, and other state and local agencies.

Houston--Office of Emergency Management. The Office of Emergency Management is an agency of the city, and is charged with responsibility for consequence management. This office can draw on the resources of the bomb squad, the Hazmat unit, SWAT, and the Houston Medical Strike Team.

Los Angeles--Terrorism Early Warning (TEW) Group. This group has a consequence management element, containing representatives from the Los Angeles Sheriff's Department, the Los Angeles City and County Fire Departments, the California National Guard, and the Los Angeles County Office of Public Safety. This group has developed plans for responding to and managing the consequences of a terrorist attack.

V. CONCLUSION

Security for our Nation's 185 deepwater seaports has gone through a dramatic evolution. Before September 11, 2001 seaport security was not a major concern, with most efforts in this area focusing on general criminal activity, physical security and access control issues. Although the port community acknowledged the threat of terrorism and a number of ideas for improving security were proposed, very few comprehensive security measures were established. Lacking any sense of urgency few of the proposed security improvements were acted upon. After September 11, the US government discovered the urgency and instituted many security changes. At the same time that numerous changes in port security were being implemented nationally by the US government, a number of important security changes were initiated by local seaports. Our report focuses on seaport security procedural and system changes initiated locally, an area receiving scant attention. While much attention emerged in 2006 due to the sale of British company P&O Ports, including its American port assets to Dubai Ports World, less attention has been given to researching specific port security measures that local ports can adopt. The controversy surrounding Dubai Ports World grabbed the headlines, because of the alleged national security risk of a foreign entity having port management responsibilities at major U.S. seaports. However, few noted the more alarming homeland security problem of the lack of answers to some fairly basic questions about improving local port security.

Our study attempted to identify the "best" and most "promising" local practices in port security, and where there was a compelling local adaptation of a federal-wide practice those were also explored. Local port security officials have had considerable experience with a number of security practices. Our report offers their valuable insights into these practices as they have been applied in 17 seaports. Our case studies of exemplary and innovative security practices in 17 seaports focused on intergovernmental and public-private partnerships and elements of success

of those partnerships. As part of our case studies and observational assessments of the ports in our study, we also interviewed a wide range of persons involved in managing the port and providing for its security. Through these methods we identified promising practices related to the five general areas of improving (1) *awareness* of threats to a port, (2) *prevention* against an attack on a port, (3) enhancing *preparedness* for an attack against a port, (4) *response* after an attack, and (5) *recovery* after an attack.

First, a considerable amount of work has been undertaken in the area of raising awareness about threats to port security in the 17 ports we visited. First, in the area of stakeholder coordination and collaboration initiatives we observed a range of awareness raising activities through the Area Maritime Security Committees (AMSC) program. AMSCs have done a good job serving as forums for local, regional and federal seaport stakeholders to gain a comprehensive perspective of port security issues. AMSCs have served as effective organizing bodies to build plans to secure seaports and coordinate efforts to raise maritime awareness of terrorism. AMSCs disseminate information through regularly scheduled meetings, issuance of electronic bulletins on suspicious activities around seaport facilities, and sharing key documents. Ports were also able to increase awareness of security threats through a variety of other committees and councils such as the Seattle - Washington State Ferry Security Committee**,** Texas City Port Security Council, the Los Angeles Port Community Advisory Committee, and the Houston Law Enforcement Subcommittee of the Area Maritime Security Committee of the Port of Houston. In addition, several ports have created other methods by which they can share information and intelligence through protocols for detecting and monitoring port related security risks and systems for enhancing intelligence sharing. Some of these best practices were port specific like Project Seahawk in Charleston, and others were broader homeland security efforts designed to protect all the vulnerable targets found in a state (e.g., the Fusion Center in Boston).

Some of the best practices for enhancing awareness that were port specific include port intelligence teams or special port security units within centers. These teams or units often collect and analyze intelligence information that may affect port security and reach out to members of the maritime community to inform them of the importance of identifying possible terrorist suspects and the need to convey that information to law enforcement officials. Another port specific best practice in this area involves the managing or structuring of information technology to raise awareness of terrorist threats. Charleston's Yard Management System (YMS) is an excellent example of a system that provides a high level of integration between security and operational data. Other examples include Savannah's Navis WebAccess system, Tacoma's Central Point of Coordination Rail Management System, and Seattle's MPS/ATLAS system. Some of the best practices for enhancing awareness that were not port specific but part of a broader homeland security effort include a number of fusion centers that address port security. Also, a variety of terrorism task forces address port security, as well as a number of anti-terrorism councils and groups.

Second, preventative measures were the most common approach we observed in the ports in our study. Prevention is a critical component of port security in that it is hoped that a strong, visible defense will deter or delay an attack. In preventing attacks against ports we identified a number of promising practices, including: (1) physical security/infrastructure at seaports, (2) protocols and processes limiting entry to seaports, (3) technology detection/inspection systems,

(4) law enforcement-related activities, and (5) interagency operational centers. Our team observed a number of promising practices in the area of physical security, including: Perimeter security; fencing, walls and other barricades; security towers and platforms; and lighting. We also learned of the importance of minimum standards in the area of physical infrastructure, and the problem of restricting waterside access to port facilities. While regular fences can be easily circumvented, a variety of security enhancements can be added to make it more difficult to circumvent a fence and protect sensitive elements in a port. We also observed innovations in sea-borne security/ floating booms and barriers in Boston and Port Everglades. Another simple strategy to deny access to shipping containers, used by most of the ports we visited, is door-to-door stacking of empty shipping containers.

Next, we observed a number of promising protocols and practices that have been established to limit entry to seaports. Although seaports have historically used conventional forms of access control such as ID badges, there is a movement now to the use of technology-intensive access control systems. For example, the pending emergence of the Transportation Worker Identification Credential (TWIC) will transform access control throughout U.S. seaports. Seaports are also turning to other types of access control devices such as biometric controls including facial, retina, iris, fingerprint, and hand geometry scans. In addition to high tech solutions, some ports have instituted some simple low-cost measures to help control access to the port. Also, some large port facilities are now requiring all personnel working or visiting the facility to travel between facility areas on a facility shuttle bus, thereby limiting access to unauthorized areas. Another development at seaports is the deployment of numerous high tech detection systems to secure the complete spectrum of seaport operations and physical assets, including: CCTVs, sensory detection systems, Non-Intrusive Inspection Technology, and Vehicle tracking systems. As with many technologies, we learned that there is still no substitute for good security procedures and well-trained human inspectors. Also, a major challenge in deploying many of these technologies at a port facility is the communication infrastructure; most ports were never designed to move video and data communications from one side of the facility, harbor or perimeter to the other. Also, with many of these systems protocols for their use are still in development and the limits of these systems are still being uncovered. Enhanced police patrol is another preventive measure being taken at seaports. These enhancements have included the hiring of additional port police officers, enhanced training, additional surveillance responsibilities, intensified random patrol and check points, enhanced collaboration with private security, the building of new port police command centers at some ports, the creation of new anti-terror and intelligence units, the switch to certified/sworn officers in some ports, the provision of new equipment to port police, and the enhancement of specialized units. We observed a number of promising examples of collaboration and interagency cooperation among law enforcement agencies at the seaports we visited. The most promising of these examples were the four interagency operational centers our team visited at the Port of Charleston (Project SeaHawk), at the Port of Miami/Port of Everglades (Project Hawkeye), Port of San Diego (Second Command Center-Joint - SCC-J), and Port of Virginia (Joint Harbor Operations Center).

Third, in enhancing preparedness for an attack against a port, we identified a number of promising practices, including: Training; field exercises; and Models, Simulations, and Games. Providing awareness training to all port personnel on security issues allows for more people to be prepared and notice something that is out of place. This is a fairly low cost best practice. We

observed a number of examples of promising practices in the area of local training in port security issues at the Ports of Charleston, Houston, Jacksonville, and Los Angeles. Another key element of preparing a port for an attack is through the use of field exercises that simulate a potential threat, attack, or incident. These exercises address scenarios such as the explosion of a "dirty bomb" that releases radioactive materials. Exercises can vary in size and scope and can test specific aspects of a terrorism response plan. Training and field exercises can involve dozens of federal, state, and local agencies including law enforcement, fire and emergency management, and a variety of other first responders. The exercise may also require close coordination across many jurisdictions, raising issues about how agency personnel can communicate effectively when they have different chains of command, communication systems, operating procedures, and equipment. Our team observed exemplary exercise programs at the Port of Savannah and Port of Jacksonville. Also, a number of the sites we visited are involved in the National Exercise Program (NEP) and the associated Top Officials (TOPOFF) National Exercise Series to increase preparedness. The ports we visited have found the NEP useful in enhancing the collaboration among port partners at all levels of government, and providing a means to conduct "full-scale, full system tests" of collective preparedness, interoperability, and collaboration. A third approach to increasing preparedness our team observed was the use of Models, Simulations, and Games (MS&G). Ports are increasingly using MS&G to better prepare first responders for how to respond to an attack against seaports. MS&G allow local officials to inexpensively plan for low-frequency, high-impact events, fits their budgetary concerns and, ideally, can disseminate information learned in large exercises to smaller entities. Some of the ports we visited have been working with games that simulate reactions to biological and radiological events, strategic incident commander games, the coordination problems associated with mass casualty medical triage, and even simulated human bodies on which to practice medical treatment. MS&G allow participants to respond as a team in real time to simulated emergency scenarios lasting two to eight hours, tracks players' responses and provides real-time assessments of their expected actions, which permits each jurisdiction to determine strengths and areas of concern in advance of a real emergency. Most interestingly, MS&G can approximate real conditions and allow personnel to "experience" dangerous events without exposing them or their environment to actual hazards, without consuming actual resources (e.g., personal protective equipment kits) and with little or no possibility of accidental injury to participants.

Fourth, we identified a number of promising practices in responding to an attack against a seaport, including: An Incident/Unified Command approach, exercise and training, and team responses. First**,** many of the ports we visited used the Incident Command System. Under this system, the agency overseeing emergency operations differs, depending on the nature and location of the event. A "Unified Command" could be established where agency managers share decision-making responsibility within a group, with individual agencies maintaining operational control for their own assets and personnel. This system allows agencies to adapt to changing situations by avoiding a rigid organizational structure, but it hinges on informal trust, cooperation, and institutional knowledge about which agency leads under what circumstances. Exercises and training programs are among the key activities that a seaport can do to prepare to respond to a terrorist attack. Under this heading, we identified a number of promising practices including Seattle's Marine Terrorism Response (MTR) Project, the Maritime Incident Resources Training Partnership (MIRT) in Boston, and local participation in the DHS developed Port Security Exercise Training Program (PortSTEP). These exercise and training programs are

intense with some combining web-based training, classroom/vessel training, and field exercises. Some provide specialized training such as responding to shipboard fires and other maritime emergencies. Many also involve cross-training with personnel across various disciplines and include governmental and private-sector officials. In responding to a terrorism incident at a seaport, the experts we talked with on our site visits also pointed to the need for strong partnerships and the formation of teams. First, the LA CERT (Community Emergency Response Team) Model stood out as a promising practice in the area of team responses. Rather than using traditional emergency response models, Los Angeles port officials have been working with the Los Angeles Fire Department (LAFD) to train civilians to be first responders in vulnerable target areas. Making use of the natural inclinations of citizens to help, the LAFD train populations in vulnerable port areas on how to help themselves and others until professional emergency response personnel can arrive at the port. Another important team response is the Maritime Safety and Security Teams (MSSTs). MSSTs serve as another resource for local seaports and are a Coast Guard rapid response force assigned to vital ports and capable of nationwide deployment via air, ground or sea transportation to meet emerging threats. MSSTs have unique capabilities, including explosive-detection dogs, personnel trained to conduct fast-roping deployments from a helicopter to a hostile vessel, and anti-terrorism/force protection. The Port of Seattle, one of our study sites, was the first port in the nation to get an MSST stationed at its port. Other promising team responses to responding to an attack are in Boston, Charleston, Houston, and Virginia. These team responses include teams of fire fighters to combat shipboard fires, emergency information centers for collating and distributing emergency information to port stakeholders, and public-private partnerships to provide specialized equipment to handle certain emergencies.

Fifth, recovery after an attack is the final key element our team explored for increasing seaport security, including the need to assure continuity of port operations to maintain vital commerce, with a focus on expediting the recovery of maritime infrastructure, transportation systems, and affected maritime communities. Compared to the other four areas already discussed, we learn about fewer promising practices in the area of recovery on our site visits. However, we did learn about promising practices in establishing recovery implementation plans in Galveston/Houston, Seattle and Los Angeles. In the Houston/Galveston area they have established Port Coordination Centers (PCCs) to inform and advise on port operational and infrastructure needs, including security concerns that arise in the case of an emergency. The Centers can convene functionally in the case of a natural disaster, or geographically, in the case of a security incident. Each PCC designates a liaison officer to the regional Port Coordination Team (PCT) in order to establish shipping priorities, manage the flow of vessel movements, preserve safety and security, and implement established emergency protocols. The PCT's role is to disseminate information concerning the nature of the threat, implement protective strategies, continue communication to update the strategies, and reopen the port in an orderly manner. Next, in Seattle the port authority has developed a business continuity plan that spells out how to decide which operations go back in business in which order. Also, at the Port of Los Angeles, the port authority has produced a business resumption plan to direct reopening of port after it has been closed due to a terrorist attack. Next, we will also talked with the participating sites about the use of a consequence management approach, involving a formal process for the restoration function after a catastrophe and addresses the ways and means to alleviate the effects of a

catastrophe. While our study sites recognized the potential value of using a consequence management approach, they had limited experience with the use of such an approach.

Providing security in and around our ports is a tremendously complicated job, requiring coordination among Federal, State, and local law enforcement agencies, as well as port authority officials, private security agencies and labor organizations. This study has identified important promising practices being used locally in 17 seaports in the U.S. to help with this complicated task. These 17 sites represent a broad range of ports with wide variation in the tonnage of cargo, the volume of containers, and the number of cruise vessels handled annually; a mixture of ports that handle cargo ships, passenger liners, and naval vessels; a mixture of landlord ports, operating ports, and limited operating ports; a variety of law enforcement structures; and reflect all major deep water locations in the US. Our study used a multi-method case study approach including conducting interviews, observing activities, collecting archival records and other files, and conducting focus groups. Our project illuminated the multitude of ways in which American seaports provide protective services, including: the multitude of public and private law enforcement and security organizations that have the authority to operate in ports and how they operate (including obstacles they have encountered and successes they have achieved), the varying organizational characteristics of these agencies, and the complexity of the inter-agency partnerships and networks that exist to provide seaport security.

Our research provides seaport officials with ideas and data to help adopt, modify or replace their security protocols, programs and other aspects of their security operations. As in many operational areas, key ingredients for successful security operations relate to port leadership, funding/resources, organizational structures that integrate security into key operational aspects of the port, communication systems and information sharing, qualified professional staff, training, team work, and clarity of mission. Other important features of port security operations include the use of incident management systems, attention to communications interoperability, public/media relations, written policies, plans and procedures, and mutual aid agreements. More specifically, the better seaport security operations often had elements of all five our general study areas of improving *awareness* of threats to a port, *prevention* against an attack on a port, enhancing *preparedness* for an attack against a port, *response* after an attack, and *recovery* after an attack.

In raising maritime awareness of terrorism, seaport officials should consider active involvement in an Area Maritime Security Committee (AMSC) or other similar committee/council to help raise maritime awareness of terrorism; developing a port intelligence team or special port security unit within an existing homeland security center, managing or structuring port data to integrate security into port operations to assure that security personnel have the necessary information they need, and working with the closest state fusion center and/or terrorism task force/council to raise the profile of port security. In preventing attacks against ports seaport officials should consider improving a range of physical security/infrastructure improvements, tightening protocols and processes limiting entry to seaports, adopting new technology detection/inspection systems, enhancing law enforcement-related activities, and fostering the advancement of interagency operational centers. While the interagency operational centers at the Ports of Charleston, Miami/Everglades, San Diego and Virginia are impressive, they are expensive and take years to become fully operational. Nevertheless, this report

documents important features at each of these centers that could be adopted individually without the development on an entire center. In preparing for an attack against a port, we identified a number of promising practices that ports should consider adopting such as port security specific training; field exercises; and Models, Simulations, and Games (MS&G). While some of these are very extensive, at least some elements of the promising practices in this area can be implemented in almost all ports. For example, awareness training to all port personnel on security issues is a low cost approach that allows for more people to notice something that is out of place. Field exercises are excellent preparatory efforts that simulate a potential attack and test aspects of the port's terrorism response plan. Similarly, MS&G can provide real-time assessments of port personnel during a simulated emergency without exposing port personnel or their environment to actual hazards, without consuming actual expensive protective equipment kits and with little possibility of accidental injury to participants.

In responding to an attack, seaport officials should consider the use an Incident/Unified Command approach to allow agencies to adapt to changing situations by avoiding a rigid organizational structure. Once again, exercises and training programs are important and among the key activities that a seaport can do to prepare to respond to a terrorist attack. Good examples of this area can be found in this report, including: Seattle's Marine Terrorism Response (MTR) Project, the Maritime Incident Resources Training Partnership (MIRT) in Boston, and local participation in the DHS developed Port Security Exercise Training Program (PortSTEP). Team responses are another critical element of an effective response to an attack against a seaport. The LA CERT (Community Emergency Response Team) Model stood out as a promising practice in the area of team responses. Other promising responses for ports to look at include team responses in the ports of Boston, Charleston, Houston, and Virginia. These promising team responses are being used help coordinate teams of fire fighters to combat shipboard fires, emergency information centers for collating and distributing emergency information to port stakeholders, and public-private partnerships to provide specialized equipment to handle certain emergencies.

In the final stage of recovery after an attack, seaport officials should consider establishing recovery implementation plans and using a consequence management approach to recovery. Compared to the other four areas already discussed, on our site visits we did not observe or learn about very many promising practices in the area of recovery. This is unfortunate, for actions such as these steps could go a long way in preserving life, property, the environment, and social, economic, and political structures, as well as in restoring order and essential services for those who live and work within the maritime domain. From our site visits our team learned about some general guidelines in coordinating recovery after an attack on a port, including: Seaport officials need to consider establishing a coordination mechanisms to oversee the entire immediate response before federal assets arrive, planning for the use of federal assets to augment the existing response, examining the role of the military's reserves in a tiered response between the first responders and the arrival of federal help, planning for surge capacities that will be needed for different types of responses, developing plans for tactical coordination at the incident, developing evacuation plans, planning for who will handle the information campaign, planning for the role of medical facilities, and ensuring that fire and police departments are prepared to work together. These are some basic steps that many ports can adopt. Recovery efforts could also be potentially advanced through the adoption of a consequence management approach.

It is our hope that this project will provide port officials with valuable information for improving their ability to provide security in and around ports, prepare for and respond to terrorism incidents, and develop partnerships that leverage the various public and private resources that may be at their disposal.

In closing, moving forward, local port security officials will need to be attentive to a number of general issues, including: the growing cost of protecting the nation's ports from a terrorist attack, balancing profits versus security concerns, integration of security into core business of port and related areas, and deciding between using private security personnel versus sworn police officers.

The growing cost of securing the Nation's port is likely to remain a major concern for the foreseeable future. The U.S. Coast Guard estimated the cost of MTSA compliance alone would be almost a billion dollars per year for a 10-year period. Debate over responsibilities in assuming costs is on-going, as "just-in-time" industry standards, finite resource allocations to DHS, and limited resources available to the ports hinder the total implementation of all measures required to ensure maximum security. The stakeholders we talked with pointed to the importance of port officials becoming staunch advocates for heightened security. They need to tout the many residual benefits that security improvements can produce, including: increased tax revenues, lower insurance premiums, and lower cargo theft. A case can also be made that the private sector should assume its share of the cost of improved port security. Manufacturers, freight consolidators, freight forwarders, and shippers should invest in providing adequate personnel to oversee the packing of containers on their loading docks. State and local governments reap the benefits of additional tax revenues generated from well-operated ports. Therefore, state and local governments are stakeholders, as well, and should assume a portion of the costs of improving port security. Significant security enhancements might also attract additional cargo traffic, thus resulting in additional profits to offset the initial security investments.

A key concern raised by the numerous port stakeholders we interviewed was the balancing of commerce and security concerns. When it comes to the operation of seaports, security and efficiency challenges are closely linked. While security is an extra step and slows the movement of cargo, the more successful ports have presented these security measures to the business community as not only a necessary step to comply with the MTSA but a service to the business community. That is, the closure of the port due to an act of terrorism would be catastrophic to the business community. This issue has surfaced around the topic of surcharges. To address security concern some ports have starting assessing security surcharge all vessels using port terminals. The surcharges are often necessary and help defray a portion of the new costs of security required by federal regulations. However, these surcharges have the potential of placing these ports at a competitive disadvantage with neighboring ports not assessing a similar surcharge. The issue of profit versus security is one that is likely to endure.

Related to this issue of profit versus security is the need to integrate security into the existing systems in place at the port. If security is seen as essential to an effective port operation it is likely to be easier to implement. Prior to September 11th, a big concern at ports was safety.

For example, at the Port of Savannah they created safety zones which were designed to protect the public from the hazards of port activity. Since September 11th, while safety is still a concern, the emphasis is on creating security zones which are designed to protect the assets and people of the port from attack. However, many of the programs designed by Port of Savannah and other ports serve a dual role of creating a safe environment for those that work and use the port and creating a secure environment. For example, good lighting not only helps catch trespassers but also helps avoid accidents. The objective is to provide for the safety and security of people, cargo and infrastructure assets while facilitating the productive flow of commerce into, within and out of the port. Another example of integrating security with port operations is the use of holistic end-to-end security solutions which include an array of data mining and access control technologies that propose to help (1) security personnel see patterns and security risks in the data that might otherwise be obscured and (2) port operations analysts improve supply chain efficiency (see Haveman and Shatz, 2006: 149-151).

Another issue for port officials to confront is the use of private security personnel versus sworn police officers. Before September 11th many ports used private security personnel or non-sworn officers to handle all port security matters. After September 11th, many ports began making the switch to certified/sworn police personnel. The decision to make the switch seems to be based on the desire for greater professionalism, accountability and improved capabilities to respond to emergencies. These may all be true, but it typically comes with a much heftier price tag. Depending on the size and activity in the port this may well be worth the extra funding. However, in some cases partnerships can be developed with nearby certified police departments to provide some of these same capabilities (e.g., the Jacksonville Sheriff's Office serves partially in this capacity for the Port of Jacksonville). Through a contractual arrangement, a private security force can be augmented by the full capabilities of a sworn police department. We believe there a number of options in this arena, each with pros and cons, which should be carefully evaluated and designed to meet the local context.

Our report also leaves open the possibility of several additional research projects. Several of the promising and innovative practices of protecting ports are in development or early-implementation phases and a continuing review of how they actually work would be very useful. For example, some of the joint command centers and information sharing initiatives could be tracked, and included in a multi-year follow up study. Also, as pointed out earlier, we designed our study to be a descriptive case study to help provide a scan of the field on the state of port security. Many of the port security practices we reviewed were too early in their development to be formally evaluated. Future studies should begin to evaluate the effectiveness of one of the more innovative port security practices identified in this and other studies.

In the end there are no magic bullets to assist the port community with the monumental assignment of protecting the Nation's port against a terrorist attack. The complex task of coordinating and working with the many involved agencies to provide the required security to our nation's seaports will not easily be accomplished. This report provided a review of innovative practices occurring at local seaports so at a minimum ports can at least start learning from each other to take on this colossal task, rather than developing new strategies from "first principles." This report shows that security improvements are being made in some seaports but that gaps in program design and implementation still remain. While much work still needs to be

done, seaports have at least made some strong in-roads into improving security. As outlined in a recent NIJ study (Davis, Ortiz, Rowe, Broz, Rigakos, and Collins, 2006 at http://www.asisonline.org/foundation/noframe/mall.pdf), it appears if the mall security community has made much less progress. Ports can learn how to fill some of these gaps by learning from the experience of the ports discussed in this report. Learning from other ports in the areas of awareness building, prevention, preparedness, response and recovery after an attack is a step in the right direction of making all of the seaports in the US safer.

References

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. 1999. *First Annual Report to the President and the Congress*. Available via the Internet at: http://www.rand.org/nsrd/terrpanel.

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. 2000. *Second Annual Report to the President and the Congress*. Available via the Internet at: http://www.rand.org/nsrd/terrpanel.

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. 2001. *Third Annual Report to the President and the Congress*. Available via the Internet at: http://www.rand.org/nsrd/terrpanel.

Agence France Presse. December 28, 2001. "Text of Bin Laden's Latest Recording on al-Jazeera." Available on the Web at indiainfo.com.

Allison, Graham. *Nuclear Terrorsim: The Ultimate Preventable Catastrophe*. New York: Times Books.

American Public Transportation Association. 2006. *Public Transportation Fact Book*. Washington, DC: American Public Transportation Association.

Benjamin, Daniel and Steven Simon. 2005. *The Next Attack: The Failure of the War on Terrorism and a Strategy for Getting It Right.* New York: Times Books.

California Office of Emergency Services. 1990. Law Enforcement Operations Report: Loma Prieta Earthquake. Sacramento: California Office of Emergency Services.

Campbell, Tanner; and Rohan Gunaratha. 2003. "Maritime Terrorism, Piracy and Crime," in Rohan Gunaratna, ed., *Terrorism in the Asia-Pacific: Treat and Response*. Singapore: Eastern Universities Press, pp. 70-88.

Clarke, Richard A. 2005. *LNG Facilities in Urban Areas: A Security Risk Management Analysis for Attorney General Patrick Lynch, Rhode Island*.

Council on Foreign Relations. 2002. *Terrorism: Questions and Answers*. Washington, DC, Council on Foreign Relations.

Davis, Mike; Kelly Mayhew; and Jim Miller. 2003. *Under the Perfect Sun: The San Diego Tourists Never See*. New York: The New Press.

Decker, Raymond J. 2002. *Seaport Security: Testimony by the Director, Defense Capabilities*

Drake, R. E., Rosenberg, S. D., Teague, G. B., Bartels, S. J., & Torrey, W. C. (2003). Fundamental principles of evidence-based medicine applied to mental health care. Psychiatric Clinics of North America, 26(4), 811-820, vii.

Ervin, Clark Kent. 2006. Open Target: Where America Is Vulnerable to Attack. New York: Palgrave Macmillan.

Essock, S. M., Goldman, H. H., Van Tosh, L., Anthony, W. A., Appell, C. R., Bond, G. R., Dixon, L. B., Dunakin, L. K., Ganju, V., Gorman, P. G., Ralph, R. O., Rapp, C. A., Teague, G. B., & Drake, R. E. (2003). Evidence-based practices: setting the context and responding to concerns. Psychiatric Clinics of North America, 26(4), 919-938, ix.

Executive Session on Domestic Preparedness, John F. Kennedy School of Government, Harvard University. 2001. Memorandum on Preparing for Terrorism: What Governors and Mayors Should Do. Cambridge, MA: Executive Session on Domestic Preparedness.

Federal Emergency Management Agency. 2001. United States Government Interagency Domestic Terrorism Concept of Operations Plan. Washington, DC: Federal Emergency Management Agency.

Flynn, Stephen. 2004. America the Vulnerable: How Our Government is Failing to Protect Us from Terrorism. New York: HarperCollins.

Flynn, Stephen. 2006. "Port Security is Still a House of Cards". Far Eastern Economic Review. January/February, pp. 5-11. See http://www/feer.com/articles1/2006/0601/free/p005.html.

Frittelli, John. 2005. Port and Maritime Security: Background and Issues for Congress. CRS Report for Congress. Congressional Research Service, The Library of Congress, Updated May 27, 2005. Washington, DC.

Greenberg, Michael D.; Peter Chalk; Henry H. Willis; Ivan Khilko; and David S. Ortiz. 2006. *Marine Terrorism: Risk and Liability*. Santa Monica, CA: RAND Corporation, Center for Terrorism Risk Management.

Groboski, David C. 1996. The Vulnerabilities of U.S. Strategic Ports to Acts of Sabotage. A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Maritime Operations. Newport, RI: Naval War College.

Harrald, John R., Hugh W. Stephens, and Johann Rene vanDorps. 2004. "A Framework for Sustainable Port Security," Journal of Homeland Security and Emergency Management: Vol. 1: No. 2, Article 12. Available at: http://www.bepress.com/jhsem/vol/1/iss/12.

Hart, Gary and Warren B. Rudman. 2002. *America—Still Unprepared, Still in Danger*. New York: Council on Foreign Relations.

Haverman, Jon and Howard J. Shatz. 2006. "Introduction and Summary," in Jon Haveman and Howard J. Shatz (eds.*), Protecting the Nation's Seaports: Balancing Security and Costs*. San Francisco: Public Policy Institute of California, pp. 1-30.

Herbert-Burns, Rupert and Lauren Zucker. 2004. "Drawing the Line Between Piracy and Maritime Terrorism," Jane's Intelligence Review, September, p. 3.

Hermann, R. C., & Provost, S. (2003). Best practices: Interpreting measurement data for quality improvement: standards, means, norms, and benchmarks. Psychiatric Services, 54(5), 655-657.

Heymann, Phillip B. 1998. *Terrorism and America: A Commonsense Strategy for a Democratic Society*. Cambridge, MA: MIT Press.

Interagency Commission on Crime and Security in U.S. Seaport*s. 2000. Report of the Interagency Commission of Crime and Security in U.S. Seaports*. 2000. Washington, DC: U.S. Government Printing Office, Fall.

Jones, Radford W.; Margaret A. Kowalk; and Patricia P. Miller. 2000. Critical Incident Protocol—A Public and Private Partnership. Michigan State University, School of Criminal Justice: East Lansing, MI.

Lehman, A. F., Buchanan, R. W., Dickerson, F. B., Dixon, L. B., Goldberg, R., Green-Paden, L., & Kreyenbuhl, J. (2003). Evidence-based treatment for schizophrenia. Psychiatric Clinics of North America, 26(4), 939-954.

Levinson, Marc. 2006. *The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger*. Princeton: Princeton University Press.

Loy, James M. and Robert Ross. 2002. "Global Trade: America's Achilles' Heel," *Defense Horizons*, February.

Major City Chiefs and Federal Bureau of Investigation. 1996. Major Incident Protocol: Reference Guide. Washington, DC: Federal Bureau of Investigation.

Manascalco, Paul M. and Hank T. Christen. 2001. *Understanding Terrorism and Managing the Consequences.* Upper Saddle River, NJ: Prentice Hall.

Merle, Renae and Spencer Hsu. 2007. "Coast Guard to Take Over 'Deepwater.'" Washington Post, p. D1, April 17.

Morrison, D. (2004). Real-world use of evidence-based treatments in community behavioral health care. Psychiatric Services, 55(5), 485-487.

Nagle, Kurt. 2002. "Port Security in the United States in the Post 9/11 Environment." A position paper of the American Association of Port Authorities. Alexandria, VA: American Association of Port Authorities.

National Commission on Terrorist Attacks Upon the United States. 2004. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. New York: W.W. Norton.

National Emergency Management Association. 2001. White Paper on Domestic Preparedness. Lexington, KY: National Emergency Management Association.

National Terrorism Preparedness Institute. 2000. Terrorism Operation Planning: Independent Study Guide. St. Petersburg, FL: National Terrorism Preparedness Institute.

Office of Inspector General, Department of Homeland Security. 2006. Review of CBP Actions Taken to Intercept Suspected Terrorists at U.S. Ports of Entry. OIG-06-43. Washington, DC: Department of Homeland Security, June.

Parnell, Gregory S.; Robin L. Dillon-Merrill; and Terry A. Breesnick. 2006. "Integrating Risk Management With Security and Antiterrorism Resource Allocation Decision Making," in David G. Kamien (ed.), The McGraw-Hill Homeland Security Handbook. New York: McGraw-Hill, pp. 431-461.

Paschall, R. 1992. *Critical Incident Management*. Chicago: University of Illinois at Chicago.

Percival, Bronson. 2005. *Indonesia and the United States: Shared Interests in Maritime Security*. Washington, DC: United States-Indonesia Society, June.

President's Commission on Critical Infrastructure Protection. October, 1997. Critical Foundations: Protecting America's Infrastructure. Washington, D.C.: President's Commission on Critical Infrastructure Protection.

Report of the Interagency Commission of Crime and Security in U.S. Seaports. 2000. Washington, DC: U.S. Government Printing Office.

Riley, Kevin Jack and Bruce Hoffman. 1995. Domestic Terrorism: A National Assessment of State and Local Law Enforcement Preparedness. Santa Monica, CA: RAND Corporation

Schmid, Alex P. and Ronald D. Crelinsten. 1993. *Western Responses to Terrorism.* London: Frank Cass.

Sherman, Rexford B. 2000. *Public Seaport Agencies in the United States and Canada*. Alexandria, VA: American Association of Port Authorities.

Sherman, Rexford B. February 5, 2003. Private interview with the Director of Research and Information Services at the American Association of Port Authorities.

Silverstein, S. M., Wilkniss, S., & Bloch, A. (2002). Best practices: don't forget the sickest patients. Psychiatric Services, 53(8), 1032-1033.

Sinai, Joshua. 2004. "Future Trends in Worldwide Maritime Terrorism," Connections: The Quarterly Journal, Vol. 3, No. 1, March, pp. 49-66.

Skinner, Richard. 2005. *Review of the Port Security Grant Program*. OIG-05-10. Washington DC: Office of Inspector General, Department of Homeland Security, January.

United States Coast Guard Port Security Directorate. *Marine Homeland Security*. Washington, DC: U.S. Coast Guard

United States Commission on National Security/21st Century. 2001. *Road Map for National Security*. Washington DC: U.S. Commission on National Security/21st Century.

United States Department of Homeland Security Office of Inspector General. 2005. Audit of Targeting Oceangoing Cargo Containers (Unclassified Summary) OIG-05-26. Washington, DC: United States Department of Homeland Security, Office of Inspector General, March 31.

United States Department of Homeland Security, Office of Inspector General. 2006. *Review of CBP Actions Taken to Intercept Suspected Terrorists at U.S. Ports of Entry*. Washington, DC: United States Department of Homeland Security, Office of Inspector General, June.

United States Department of Transportation . September, 1999. "An Assessment of the Maritime Transportation System: A Report to Congress. Washington, DC.

United States General Accounting Office. 2002a. *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful*. Statement of JayEtta Z. Hecker, Director, Physical Infrastructure Issues, GAO. "Statement Before the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform. GAO-02-993T. Washington, D.C, August 5.

United States General Accounting Office. 2002b. *Combating Terrorism: Actions Needed to Improve Force Protection for DOD Deployments through Domestic Seaports*. GAO-03-15. Washington, D.C.: U.S. General Accounting Office, October.

United States General Accounting Office. 2004. Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, "Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection," Statement of Richard M. Stana, Director, Homeland Security and Justice Issues. GAP-04-557T, March 31.

United States Government Accountability Office. 2003. *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*. GAO-03-770. Washington, DC: U.S. Government Accountability Office.

United States Government Accountability Office. 2004. *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*. GAO-05-106. Washington, D.C.: U.S. Government Accountability Office, December.

United States Government Accountability Office. 2005a. *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security*. GAO-05-404. Washington, DC: U.S. Government Accountability Office, March 11.

United States Government Accountability Office. 2005b. *Maritime Security: New Structures Have Improved Information Sharing, But Security Clearance Processing Requires Further Attention*. GAO-05-394. Washington, DC: U.S. Government Accountability Office, April 15.

United States Government Accountability Office. 2005c. *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts*. GAO-05-557. Washington, DC: U.S. Government Accountability Office, April 26.

United States Government Accountability Office. 2005d. *Maritime Security: Enhancements Made, But Implementation and Sustainability Remain Key Challenges*. GAO-05448T. Washington, DC: U.S. Government Accountability Office, May 17.

United States Government Accountability Office. 2005e. Testimony Before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate. "Homeland Security—Key Security Programs Can Be Improved," Statement of Richard M. Stana, Director, Homeland Security and Justice Issues. GAO-05-466T. Washington, DC: U.S. Government Accountability Office, May 25.

United States Government Accountability Office. 2005f. *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*. GAO-06-91. Washington, DC: .U. S. Government Accountability Office, December.

United States Government Accountability Office. 2006. *Maritime Security: Information-Sharing Efforts Are Improving*. GAO-06-933T. Washington, DC: U.S. Government Accountability Office, July 10.

United States Government Accountability Office. 2007. "Maritime Security: Observations on Selected Aspects of the SAFE Port Act." Statement of Stephen L. Caldwell, Director, Homeland Security and Justice. Testimony Before the Subcommittee on Border, Maritime, and Global Counterterrorism; Committee on Homeland Security; House of

Representatives. GAO-07-754T. Washington, DC: U.S. Government Accountability Office, April 26.

United States Maritime Administration. 2005. *U.S. Public Port Expenditure Report*. Washington D.C. U.S. Department of Transportation; Maritime Administration; Office of Ports and Domestic Shipping.

Yin, R. (1994). *Case study research: Design and methods* (2nd ed.). Beverly Hills, CA: Sage Publishing.

APPENDIX A
POLICE EXECUTIVE RESEARCH FORUM/DOJ PORT SECURITY PROJECT SITE VISIT PROTOCOL AND PROCEDURES

Purpose of Study

The purpose of the study is to determine, examine and explicate the various methods being used to protect America's ports against terrorist attacks.

Site Visit Objectives

The purpose of the case study site visits will be to determine:

1. How protective steps vary across port size and type, region, port organizational structure, and policing approach;
2. How public law enforcement agencies and private security collaborate to provide security;
3. The challenges faced and resources available in providing security;
4. The strategies and tactics used to provide security; and
5. The most promising practices and lessons learned.

Site Selection Criteria

Sites will be selected with the following criteria in mind:

1. They should represent ports with wide variation in the tonnage of cargo, and the volume of containers, and the number of cruise vessels handled annually;
2. They should represent a mixture of ports that handle cargo ships, passenger liners, and naval vessels;
3. They should represent a mixture of landlord ports, operating ports, and limited operating ports;
4. They should represent a variety of law enforcement structures: port authority police agencies, port authority security departments, reliance on local law enforcement, and contracted law enforcement;
5. They should reflect all major deep water locations (the Atlantic Ocean, the Pacific Ocean, and the Gulf of Mexico); and
6. They should be willing to cooperate with the provisions of the study.

For budgetary reasons, we will seek to select sites in geographic clusters, allowing us to visit more than one port per trip.

Pre-Visit Activities

Making Arrangements for Site Visits. Once a preliminary list of approximately 20 sites is created, the research team will send e-mail messages to the Captains of the Port (COTP) responsible for each those sites (in some cases, the COTP may be responsible for more than one

of the ports). We will also send e-mail messages to the chief(s) of the municipal law enforcement agency/agencies in the vicinity of the port as well as the person in charge of security for the port, as designated by the American Association of Port Authorities. In these e-mails, we will explain the nature of the NIJ-funded project, list the members of our advisory board, explain that the board suggested that their port be a part of the study, and solicit the respondent's cooperation in the study. We will point out that, under strictures of Federal law, no port or individual will be identified. Finally, we will indicate that we will be calling them in the next several days to provide further information about the study, answer any questions, and begin to make arrangements for a site visit.

Within a week after sending the e-mail, a senior staff member will call the recipients of the e-mails to answer any questions and to encourage participation in the study. If consent to participate is received, we will begin to make arrangements to make a site visit. We will also request copies of any written material that would provide background about the port and its security. We will, further, elicit recommendations concerning other persons involved with providing security at the port whom we should contact.

Based upon the recommendations provided during the follow-up telephone calls, we will make telephone calls to potential interview subjects to make arrangements for an interview during a site visit.

Comprising the Site Visit Team. Site visits will, whenever possible, be made by teams of two members of the project staff. The senior staff member will be designated as the lead person in the team.

Preparing for Site Visits. Prior to conducting a site visit, site visit team members will review all relevant materials specific to the site, including the information sent by the COTP and other information available in public sources.

Conferring with the Designee(s). As soon as possible after receiving permission to proceed, a senior staff member will contact the designee(s) selected by the Captain of the Port. The purposes of this call will be to:

- Negotiate the timing of the site visit;
- Brief the designee(s) concerning the nature and purposes of the site visit;
- Request that the designee provide names and contact information assist in developing an agenda for the visit and arrange interviews with those persons listed under "Conduct Interviews" in the "Conducting the Site Visits" section below.

Pre-Visit Confirmation. Prior to the visit, the site visit team will confirm by e-mail and/or telephone with the designee(s) and the others to be interviewed of the nature and timing of the visit.

Conducting the Site Visits

Site visits are expected to last from three to five workdays, depending upon the number of persons interviewed and the programs to be observed, and the complexity of the local situation. In each site visit, the following tasks will be performed.

Conduct Interviews. In order to accomplish the objectives of the site visits, members of the site visit team will interview a wide range of persons involved in managing the port and providing for its security. In all sites, persons interviewed would include, but not necessarily be limited to, the following, or their representatives:

- Captain of the Port and other US Coast Guard representatives;
- Port Authority Manager/Director;
- Port Security Director;
- Facility Security Officers;
- Port Authority Police Chief (if any) and officers;
- Representatives of local municipal, county, and state police agencies involved with port security;
- Representatives of other federal government agencies involved with port security, including FBI, US Navy, DEA, and ICE.
- Representatives from private security agencies, if appropriate;
- Representatives of local fire departments;
- Representatives of tenants in the port, if appropriate;
- Representatives of unions and stevedores; and
- Others, as identified.

Before conducting any interview, project staff will inform the interview subject that, because the study if funded with a DOJ grant 1) the identify of the person and the port will be kept strictly confidential; 2) all information collected will be coded and kept in a secure location, with access only to project staff members on a need to know basis; 3) the subject and the port will be able to review the draft report for accuracy and security concerns prior to its completion; and 4) participation is voluntary and can be terminated at any time.

Collect Archival Data. In addition to material reviewed before making the site visit, members of the site visit team will collect and examine other archival documents, including:

- Port descriptive materials;
- Port annual reports; and
- Other material relevant to port security.

Observe Programs. Where feasible, members of the site visit team will conduct observations of security programs, operations, and exercises in action at or around the port.

Focus of Activities on Site

The site visit team will address the following issues:

- What is the management structure of the port? Does it operate as a landlord port, an operating port, or a limited operating port?
- Is there a Port Authority police department?
- Is there a Port Authority security department?
- What are the primary security concerns in and around the port?
- Has the port security plan(s) been completed? Who produced it/them? To what extent has the plan/have the plans been reviewed, approved, and implemented?
- What agency/agencies are responsible for providing security at the port? How are their efforts coordinated?
- What is the nature of the relationship among the principal stakeholders involved in providing security—port authority police, municipal police, county law enforcement agencies, other government agencies, and private security?
- Do local law enforcement and/or private security participate in the maritime security committee? Do other law enforcement agencies? Private security?
- What sources of intelligence do local law enforcement and/or private security have with regard to security threats? Is it shared with other agencies? Which other agencies?
- Who is represented on the Maritime Regional Security Committee (or its equivalent)? How often does it meet? What role does it play?
- Do local law enforcement agencies and/or private security work with the local Joint Terrorism Task Force?
- Do law enforcement agencies and/or private security assist in conducting background checks conducted for personnel working at the port? For what type of workers? By whom? What are the criteria for employment?
- Do law enforcement agencies and/or private security patrol the perimeters of the port—landside and seaside?
- Do law enforcement agencies and/or private security enforce access control for entry to the port?
- Do law enforcement and/or private security require credentials for persons entering the port? What type of information is contained on these credentials? Are different types of credentials required for different types of people entering the port?
- Do law enforcement and/or private security inspect containers and other cargo coming into and leaving the port? Do law enforcement and/or private security secure the public spaces within the port?
- Are law enforcement and/or private security responsible for access control to separate terminals within the port?
- Do law enforcement and/or private security limit access to certain parts of the port to people with special credentials?

- What training regarding port security has been provided to law enforcement and private security? How many hours? By whom? To whom? What was the nature of the training? Do you feel it is sufficient?
- What plans exist concerning how to respond to a terrorist attack if it actually occurred? Have you conducted exercises to practice implementing those plans? How many? With whom?
- What plans have been made to mediate the effects of a possible attack? What roles are to be played by which agencies?
- What plans have been made to restore the port to operational condition?

Post-Visit Activities

To the extent possible, team members will document their observations and interview notes during the site visit. They will compare their observations throughout the visit. As soon as possible after the visit, they will type and exchange their field notes. All notes will be coded and kept in a secure location accessible only to key project staff members. Copies of site visit summaries will be sent to site representatives for their review and comment.