REPORT OF THE INTERAGENCY COMMISSION ON CRIME AND SECURITY IN U.S. SEAPORTS

FALL 2000

Table of Contents

Executive Summary

On April 27, 1999, President Clinton signed an Executive Memorandum directing the establishment of the Interagency Commission on Crime and Security in U.S. Seaports. Citing both the importance of seaports to the nation's commerce and the presence at seaports of crime and conspiracies associated with those crimes that "pose threats to the people and critical infrastructures of seaport cities," the President called for "a comprehensive review of the nature and extent of seaport crime and the overall state of security in seaports, as well as the ways in which governments at all levels are responding to the problem."

The Executive Memorandum directed that the Commission's report include the following:

- 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.
- Recommendations for improving the response of the federal, state, and local governments to the problem of seaport crime.

This executive summary presents the Commission's key findings and all of its recommendations in response to the President's mandate.

Crime at U.S. Seaports

The Commission was not able to determine the full extent of serious crime at seaports. No national data collection and reporting systems are now in place that cover serious crime in seaports. Federal agency databases do not adequately collect and report crime data by seaports, and state and local law enforcement agencies do not specifically collect and report crime data by seaports. For these reasons, the crime data summarized in this report, while significant, do not offer a fully comprehensive picture. Serious crime at seaports is probably more extensive than what is detected, reported, and retrievable from federal, state, and local law enforcement agencies.

Criminal activity with a nexus to U.S. seaports encompasses a broad range of crimes, including the importation of illicit drugs, contraband, and prohibited or restricted merchandise; stowaways and alien smuggling; trade fraud and commercial smuggling; environmental crimes; cargo theft; and the unlawful exportation of controlled commodities and munitions, stolen property, and drug proceeds.

While it is difficult to develop a complete picture of all crimes extant in seaports because of venue, reporting definitions, and collection issues, it is possible to look at available reports as indicators to make diagnostic conclusions. Significant criminal activity is taking place at most of the 12 seaports surveyed by the Commission and was not limited to a few specific seaports. The primary criminal activity at seaports is in violation of federal laws, much of it directly related to the importation and

exportation of goods and contraband. Federal agencies are primarily responsible for contraband and alien interdiction. State and local law enforcement agencies support federal anti-smuggling efforts, but focus primarily on violent and property crimes on seaport premises.

Drug smuggling is the prevalent crime problem reported at seaports. Cocaine is the principal illicit drug smuggled into the United States through seaports, but significant quantities of marijuana are also smuggled. Most illicit drugs enter through commercial traffic, particularly in containers, but some also enter on commercial vessels and passenger cruise ships, concealed by crewmembers and passengers. Smuggling by crewmembers is a particular problem at seaports where bulk cargo is imported.

Internal conspiracies present the most serious challenge to drug interdiction efforts at seaports because they can thwart traditional Customs Service targeting and examination processes. These conspiracies are criminal activities committed by smugglers or other organized criminal groups aided by corrupt individuals employed in seaports or within the transportation industry. They were reported at 9 of the 12 seaports the Commission surveyed. Drug smuggling organizations use transportation industry employees with access to seaport areas, and/or with specific knowledge of Customs procedures, to facilitate their drug smuggling operations at seaports by controlling and monitoring drug shipments concealed inside cargo shipments of legitimate importers. These internal conspiracies play a substantial role in facilitating drug smuggling and present a major investigative challenge to interdiction efforts.

Stowaways and alien smuggling are the largest problems facing the Immigration and Naturalization Service in seaports. At 10 of the 12 seaports surveyed it is stowaways. However, organized alien smuggling has also surfaced as a major concern, particularly on the West Coast. In the first half of fiscal year 2000, there were more apprehensions of smuggled aliens than for the three years for which the Commission gathered crime data.

Trade fraud offenses were reported at 9 of the 12 seaports surveyed. Most nondrug import crimes go undetected at seaports because less than 2 percent of the cargo is inspected. Trade fraud includes diversion of imported or in-bond merchandise into the commerce of the United States; textile transshipments to avoid quotas; undervaluation, double invoicing, or false description of merchandise imported into the United States; importation, transportation, and distribution of counterfeit goods subject to trademark and copyrights; and importation, transportation, and transshipment of items that pose a threat to U.S. consumers or the environment, including tainted or prohibited foodstuffs, medicines, unapproved drugs, and chlorofluorocarbons. Environmental offenses were reported in 8 of the 12 seaports surveyed.

Cargo theft offenses or recoveries were reported at 7 of the 12 seaports surveyed. The vast majority of cargo thefts occur outside of the seaports in the metropolitan areas. Neither industry nor the law enforcement community has been able to provide a valid estimate of the severity of the cargo theft problem for two reasons. The first is that cargo crime is not a specific reportable offense in the Uniform Crime Reporting Program. Adding it to a national reporting system, such as the Uniform Crime Reporting Program or the National Incident-Based Reporting System, would help law enforcement authorities assess the extent of losses and develop appropriate responses to the problem, and would also increase state and local law enforcement authorities' awareness of the crime. The second reason is the reluctance of the private sector to report cargo theft to law enforcement authorities. The private sector is chiefly concerned with rising insurance premiums, competitiveness within the industry, and reputation for reliability. The

most effective law enforcement efforts to combat cargo thefts are task forces comprised of state, local, and federal agencies, which are specifically trained and dedicated to attacking cargo theft.

Export crime is perpetrated to avoid the United States' controls on the export of strategic and sensitive items including munitions and firearms, weapons of mass destruction-related materials and components (such as chemical precursors and biological agents), missiles, critical technologies, military hardware and equipment, critical dual-use items, and monetary instruments. Outbound currency seizures were reported at 6 of the 12 seaports surveyed. The three largest outbound currency seizures ever made by Customs have been in seaports. A shipper's export declaration is required for most goods. But many filings are vague and incomplete, only half are filed electronically, and most are filed after the vessel has departed. Data are not available to assess the extent of export crime at U.S. seaports. However, export crime statistics for the 12 seaports surveyed covering the period 1996-1998 suggest that the export of stolen vehicles is the most detected export crime at the seaports, followed by export crime involving controlled commodities and munitions.

Stolen vehicle exports were reported at 10 of the 12 seaports surveyed. The National Insurance Crime Bureau reports that more than 200,000 stolen automobiles, totaling $4 billion in value, are illegally shipped out of the United States each year.

Other serious crime, covering offenses such as bribery, public corruption, extortion, and racketeering, was reported at 5 of the 12 seaports surveyed. The extent of these crimes is hard to determine because they are difficult to identify and expose, but most law enforcement officials agree that they do occur at seaports.

A full assessment of crime in U.S. seaports is addressed in Chapter 3 of the complete report.

Threat Posed by Terrorism

Although seaports represent an important component of the nation's transportation infrastructure, there is no indication that U.S. seaports are currently being targeted by terrorists. The FBI considers the present threat of terrorism directed at any U.S. seaports to be low, even though their vulnerability to attack is high. The Commission believes that such an attack has the potential to cause significant damage. Some port organizations expressed frustration with not being made aware of specific threat information on an ongoing basis.

Combating terrorism can be divided into three fundamental activities: crisis management, consequence management, and protective measures. National-level responsibilities for crisis and consequence management are clearly delineated in Presidential Decision Directives 39 and 62. Responding to terrorism is a multidisciplinary effort that involves prevention of potential acts, investigation of acts that do occur, and crisis and consequence management. Therefore, a comprehensive response to terrorism involves the efforts of law enforcement and intelligence agencies, emergency response agencies, and, when necessary, even the military. A full assessment of the threat of terrorism in U.S. seaports appears in Chapter 4 of the complete report.

The State of Security of U.S. Seaports

The state of security in U.S. seaports generally ranges from poor to fair, and, in a few cases, good.

There are no widely accepted standards or guidelines for physical, procedural, and personnel security for seaports, although some ports are making outstanding efforts to improve security. Control of access to the seaport or sensitive areas within the seaports is often lacking. Practices to

restrict or control the access of vehicles to vessels, cargo receipt and delivery operations, and passenger processing operations at seaports are either not present or not consistently enforced, increasing the risk that violators could quickly remove cargo or contraband. Many ports do not have identification cards issued to personnel to restrict access to vessels, cargo receipt and delivery operations, and passenger processing operations.

At many seaports, the carrying of firearms is not restricted, and thus internal conspirators and other criminals are allowed armed access to cargo vessels and cruise line terminals. In addition, many seaports rely on private security personnel who lack the crime prevention and law enforcement training and capability of regular police officers.

Frequently, federal, state and local law enforcement agencies do cooperate with each other in regard to security matters, including the sharing of intelligence. However, there were locations surveyed where private sector representatives said they were unclear which federal agency required reports of possible cargo thefts and other violations. No regular security-related local meetings are being held between law enforcement organizations (federal, state, and local), the trade, and port authorities, with the exception of those relatively few Strategic Seaports where Port Readiness Committees are active.

Visits to 4 of the nation's 13 commercial Strategic Seaports, which are critical chokepoints for future military mobilizations, found that the National Port Readiness Network/local Port Readiness Committee concept is fundamentally sound, but in need of increased emphasis and support. Specific problems included inadequate proactive local planning for military mobilization security, a lack of actual port readiness exercises, an absence of vulnerability/threat assessments for those seaports, and a lack of specific security standards.

The Commission developed a methodology to evaluate the various ports. This became the basis for the Model Port included in Appendix F, which could become the framework for discussions on general guidelines for security at seaports.

BORDER CONTROL AT U.S. SEAPORTS

Effective controls on the arrivals of passengers, crew, and cargo can substantially reduce terrorist and other criminal threats at seaports.

Cruise ship passenger controls. The level of passenger security in place at terminals that serve cruise lines indicates a commitment to security. Terminals uniformly employ private security forces, who appear to know which police unit should be notified when there is a problem. Security procedures are, for the most part, well coordinated between terminal and vessel personnel in the case of passengers boarding to depart the United States. However, the arrival of international passengers is marked by facilities that allow direct access to uncontrolled areas where disembarking passengers and their baggage intermingle with visitors, baggage handlers, truck drivers delivering stores to ships, and dock workers—many of whom may not have been cleared by anyone for access to those areas. Separation of arriving passengers and baggage could be accomplished by facilities dedicated to passenger control and examination following Federal Inspection Services guidelines.

Import control. More than 600 laws and 500 trade agreements must be checked for applicability on each import. Sixty separate federal agencies have an interest in inspecting merchandise. Customs is the agency with the largest presence for cargo

inspection in seaports; Agriculture is second.

Given the immense volume of cargo, without automated assistance, a difficult task would certainly be impossible. In 1982, Customs implemented the Automated Commercial System, which allows importers to file import documentation and pay duties electronically. The collection, analysis, and dissemination of usable cargo information are essential to protecting U.S. border ports. However, the Automated Commercial System is now outdated and relies on inadequate or inaccurate information. Criminals can bypass the federal clearance and inspection process through underreporting, misreporting, or not reporting at all. Information on ships' manifests is often wrong or incomplete. Import entry documentation contains more information than the manifest, but it is not required for at least five days after arrival. Violators have exploited the in-bond system for moving imported cargo across the country for export from a different port; they divert or substitute cargo, evade duties, or smuggle unlawful merchandise. These issues need to be addressed.

Violations of regulations on imports of foreign food and the introduction of foreign insect species raise concerns about imports that can affect the nation's food supply. U.S. agricultural interests have suffered major losses as a result of infusions of foreign insects and plant species. Concerns have also been raised about the safety of food imported through seaports.

An unintended consequence of increasing automation is that federal inspectors are more often behind computers than on the docks. This creates opportunities for criminal enterprises to take hold. Many stakeholders told the Commission that more federal inspectors were needed at the docks. An alternative would be mobile computer systems that provide inspectors with timely information and free them from their office computer terminals.

Location of federal inspection facilities. Federal inspection facilities should be located at the docks rather than in remote private sector locations. And federal inspection agencies should be co-located in joint facilities so that they can share equipment, reduce costs, and coordinate enforcement and compliance examinations.

Export control. The law and regulations for exports are different from those for imports. Recent advances in the Automated Export System have increased filing of shipper's export declarations via automation to almost 50 percent, but the delayed filing privilege allows most goods to depart the country before information is available to control agencies. The inspection and criminal investigation personnel resources devoted to export transactions are only a small fraction of those devoted to imports. Customs and the Commerce Department are the agencies with preeminent roles.

Seaports are vulnerable to those trying to acquire or sell U.S. goods illegally. Some of these goods, such as weapons, munitions, and critical technology, affect the national security. Other crimes, such as diversion into the U.S. economy of foodstuffs that had been denied entry into the country, affect public health.

A full assessment of the state of security in U.S. seaports appears in Chapters 5 and 9 of the complete report.

Roles and Authorities in Seaports

The 361 U.S. seaports range widely in size and characteristics. The most basic economic activity at seaports is effecting the transportation of cargo. The regulatory framework of U.S. seaports, which began their existence in this country before there was a national government, evolved very differently from that of other entities such as airports. The United States has no

national port authority. The federal, state, and local governments share jurisdiction over ports and harbors. The primary responsibility rests with the states, which charter seaports within their territories. A port authority is an instrumentality of state or local governments. Some marine terminals are operated by public port authorities, others by private sector tenants of the port authority. Other facilities are wholly independent of the state. The Commission found that it is very different in each seaport.

The Second Act of Congress in 1789 established the Customs Service and its ports of entry, with a mission of being present at every unlading of a vessel in order to conduct a complete inventory of the cargo, appraise the value, and collect the applicable duty as well as tonnage taxes and fees. The Coast Guard was established in 1790 as the Revenue Cutter Service to enforce the nation's customs laws on the seas. The roles of both agencies have expanded greatly through the years. Among many other federal agencies that play important roles at seaports are the Department of Agriculture, the Immigration and Naturalization Service, the Drug Enforcement Administration, the Federal Bureau of Investigation, the Food and Drug Administration, the Environmental Protection Agency, and the Department of Commerce. The Department of Defense, through the Maritime Administration, has port planning orders in place at 13 commercial seaports (designated as Strategic Seaports), which identify tentative arrangements for the use of facilities and services needed for military deployments.

State and local governments, as well as all levels of law enforcement, have important roles. Among the major stakeholders of seaports are the port authorities, vessel operators/carriers, terminal operators, trucking companies, warehouse or container freight station operators, railroads, importers and exporters, freight forwarders, cruise line operators, contract security forces, labor groups and dock workers, and trade associations.

A more detailed overview of missions and authorities appears in Chapter 2 of the complete report.

Nature and Effectiveness of Coordination

The threat warning systems designed to relay specific information from the federal sector to the private sector appear to be satisfactory and operating as intended. Partnership programs have been very successful and are a force multiplier for federal agencies. However, policing and security functions are fragmented at many seaports, and coordination is lacking among the various police and security personnel. There is a disparity in substantive knowledge, training, and capability in port security and law enforcement matters between the local police (including port police) and contract security personnel at many ports that were surveyed. At some seaports there is an apparent mistrust of, and lack of cooperation between, labor and law enforcement agencies.

Cooperation among law enforcement agencies. The Commission found that coordination and cooperation among federal, state, and local law enforcement agencies is good at the 12 seaports surveyed. The nature and extent of coordination efforts encompasses a wide variety of criminal activities, among a range of law enforcement agencies. The varied coordination efforts included drug smuggling, health and safety crimes, stolen vehicles and cargo theft, environmental crimes, and export control crimes. Some of the coordination efforts were solely among federal law enforcement agencies; other efforts included federal, state, and local law enforcement agencies.

Although much of the crime at seaports involves violations of federal laws relating

to the importation and exportation of goods, most of the state and local law enforcement agencies support anti-smuggling efforts. Some of the most successful law enforcement efforts were at seaports where multiagency task forces of federal, state, and local agencies addressed specific crime problems. Few seaports, however, have stand-alone task forces where agencies routinely meet to discuss approaches to all types of crime, rather than a specific crime, and to assess threats to the seaport. Additional resources allocated by law enforcement agencies might increase participation in task forces and other effective interagency partnerships and initiatives involving federal, state, and local law enforcement agencies and might also enhance cooperation, coordination, and responses to seaport crime.

Role of port officials. Some commercial port officials either were unaware of the nature and extent of crime being committed at their seaports or considered most of the criminal activity related to the importation and exportation of goods, where there was no immediate victim in the port, to be the responsibility of the federal government.

Role of security. Inadequate security at seaports contributes to criminal activity. Many law enforcement officials believe that security enhancements are essential in the long run to combat internal conspiracies, smuggling by crewmembers, alien smuggling, and cargo theft, while reducing the vulnerability of critical seaport infrastructure, and increasing the effectiveness of the federal government's border control functions.

A full assessment of the nature and effectiveness of ongoing cooperation among federal, state, and local agencies appears in Chapter 6 of the complete report.

ADDITIONAL MATTERS

In addition to addressing the tasks contained in the Executive Memorandum, the Commission found that three important enablers—technology, intelligence and information management, and international cooperation—warrant specific focus.

Technology

While using technology is only one means to an end and not the end itself, adding the right technology at U.S. seaports can: (1) increase the effectiveness, efficiency, and safety of port operations and the enforcement of applicable laws and regulations; (2) decrease vulnerabilities to criminal activities; (3) serve as a force multiplier for port operators and enforcement agencies; (4) provide new capabilities for port security and control; and (5) facilitate quick responses for military mobilization, terrorist threats, and new requirements.

An extensive review of technology already available and under development for use in the next five years finds that viable technology exists for purposes of security, investigation, and contraband detection. Some of this technology is already in place; some is being developed; much could be adapted to meet the needs that the Commission has identified at seaports. A joint effort by federal inspection agencies to develop a five-year plan identifying technology needs, priorities for deployment, and funding sources is essential. The application of technology needs to be addressed across the agencies in seaports on a continual basis.

A more detailed list of available technology is included in Appendix E, and further discussion is in Chapter 5 of the complete report as well.

Intelligence and Information Management

The Commission heard concerns from law enforcement agency personnel and maritime industry focus groups that informa-

tion needed for seaport security was lacking in three principal areas: (1) availability to law enforcement agencies of relevant, actionable intelligence on seaport crime; (2) awareness of terrorist threats and availability of threat information to the private sector as well as to inspection personnel at seaports; and (3) integrated information on the movement of vessels, people, and cargo within seaports and ready availability of that information to government agencies and private sector security organizations.

Collecting, analyzing, and disseminating intelligence is central to effective efforts to counter seaport crime. Predictive, operational intelligence of a quality that provides explicit information that is usable at the tactical level can increase the probability that certain threats can be identified and, if appropriate, interdicted before arrival in U.S. ports and container or other inspections will result in contraband seizures and arrests. Development of intelligence sources, overseas and at home, is critical.

Exchange of information on terrorist threats, criminal activities, and port security among law enforcement agencies and the private sector is also critical. Multiple federal agencies distribute terrorist threat information to a variety of end users, each targeting different customers. These processes appear to be working well, with end users gaining access to terrorist threat information through the most appropriate channels. Therefore, it does not appear necessary to centralize the distribution of this information within a single federal agency, or to incorporate terrorist threat dissemination procedures for seaports into regulation.

Problems persist, though, with getting more general information on crime and security trends into the hands of the security personnel at the ports who must implement enhanced security measures. In many cases this is a lack of internal communication between the private sector and law enforcement agencies at the ports. Increasing the awareness of security-related threats among port facilities and vessel operators, and expanding the availability of threat information from government sources through training, outreach, and public/private interagency forums, such as local port security committees, would do much to alleviate this problem.

Finally, the information systems that support decision-making need attention. The Customs information management and processing systems are of critical importance. These underlying systems process the electronic equivalent of millions of documents and forms that are associated with the importation, movement, and clearance of hundreds of billions of dollars of commercial cargo. They must be strengthened to accommodate the ever-increasing demands of international trade. It is important not only that robust electronic data processing systems are maintained, but that such systems continue to evolve and develop to reflect the changing trade environment and interagency enforcement and compliance priorities. The Automated Commercial Environment plan of the Customs Service is a step in that direction.

The issues of intelligence and information management are more fully addressed in Chapter 7 of the full report.

International Cooperation

International commerce has changed dramatically since the end of the Cold War. Globalization and the liberalization of trade practices have resulted in fewer impediments to trade and an increase in the flow of goods, most of which are transported by sea. Advances in technology and communications have changed the way companies conduct business. More companies have become global in nature. International competition, open markets, and the dropping of trade barriers contribute to the selection of goods available to U.S. consumers and producers. Developed nations like the United States are increasingly dependent on for-

eign markets to produce goods through cheaper manufacturing costs.

The security of foreign seaports has a direct influence on the security of U.S. seaports. Shipping and cargo originating in or transiting foreign ports provide an avenue for the introduction of transnational threats to the United States. Increased involvement overseas by U.S. law enforcement agencies engaged cooperatively with their foreign counterparts is essential to proactive policing of international cargo crime and to improving the results of law enforcement efforts.

International cooperation can be critical in addressing many of the issues that are the focus of this report. The susceptibility of U.S. ports to the repercussions of lax security in foreign ports, for instance, makes international port security engagement a priority.

The issue of international cooperation is more fully addressed in Chapter 8 of the complete report.

FINDINGS AND RECOMMENDATIONS

The Commission recommendations set forth below have significant crime control and other national security implications. Substantial resources will be required to implement many of them. These resources may be reprogrammed from within a department's base funding, or new resources in addition to base funding. The Commission urges that the findings and recommendations of this report be accorded prominence for agency policy, program, budget, and regulatory purposes. To the extent that the recommendations have resource implications, the Commission recognizes that they must be weighed against other priorities in the context of the overall budget process.

There are many more specific findings contained in Chapters 2 through 8 of the complete report. The key findings that drive the recommendations are summated here. The recommendations are numbered in the sequence that they appear in the report.

Finding 1. Notwithstanding the existence of a series of Presidential Decision Directives, as well as various national strategies and other directives with application to security in seaports, there exists a need for a more comprehensive and definitive statement of the specific federal responsibilities in this context. Moreover, this statement should be disseminated broadly, particularly to the local levels at which most security activities and operations are undertaken.

Recommendation 1. Strengthen interagency, intergovernmental, and public/private sector efforts to address the threats of seaport crime (including terrorism), and to enhance control of imports and exports through seaports. Unless otherwise specified in Presidential Decision Directives and other policy documents, lead agencies to initiate action and promote increased cooperation should be as follows: Customs, for international cargo and related contraband smuggling; Immigration, for admissibility of international passengers/crew and alien smuggling; Coast Guard, for seaport security; and FBI, for counter-terrorism.

Finding 2. Most persons who consider the significance of seaports within the larger community see them as vehicles to promote economic growth. Attention to seaport security is insufficient in part because dissemination to the local levels of what national efforts are underway, and how security can reduce crime and terrorism vulnerabilities, is lacking.

Recommendation 2. Strengthen the efforts of the Marine Transportation System national organizations to enhance the awareness of state and local governments

and private sector interests (including labor) of the vital role that seaports play in national security that extends beyond their indispensable contribution to the nation's economy.

Finding 3. The Commission was not able to determine the full extent of serious crime at seaports. No national data collection and reporting systems now in place cover serious crime in seaports. Federal agency databases do not adequately collect and report crime data by seaports, and state and local law enforcement agencies do not specifically collect and report crime data by seaports. While significant, the crime data summarized in this report do not reflect the full extent of the problem; serious crime at seaports is probably more extensive than what is detected, reported, and retrievable from federal, state, and local law enforcement agencies.

Recommendation 3. Modify, to the extent feasible, the existing databases of federal agencies with significant regulatory and enforcement missions at seaports to ensure the collection and retrievability of data relating to crime with a nexus to seaports.

Finding 4. Cargo theft is a major concern to the private sector entities that operate at seaports. Although the vast majority of the reported cargo thefts take place while shipments are outside of the seaports in the metropolitan areas, seaports provide central locations where organized crime groups can locate and easily target a wide variety of high value goods. The lack of a national collection and reporting system for cargo theft data and the underreporting of cargo theft losses by the private sector hinder the assessment of the problem and the development of appropriate solutions.

Recommendation 4. Evaluate the feasibility of capturing data on cargo theft offenses (including cargo thefts taking place outside of seaports) through the National Incident-Based Reporting System. The Criminal Justice Information Services Advisory Policy Board should take the lead in the development, management, and continued evaluation of cargo theft to facilitate the data collection required to assess the nature and extent of cargo theft reporting and facilitate databasing. This will ensure that such information provides the maximum utility to its intended users.

Finding 5. Coordination and cooperation among federal, state, and local law enforcement agencies could be improved at seaports by more joint efforts with a seaport focus. Comprehensive interagency crime threat assessments, which currently are not conducted at seaports, offer one such opportunity. By preparing annual crime threat assessments, federal, state, and local law enforcement agencies would develop a better understanding of the overall crime threat at each seaport and also lay the groundwork for enhanced communication, cooperation, and coordination.

Recommendation 5. Prepare, on an annual basis, comprehensive interagency crime threat assessments for seaports with international trade to support coordinated operational planning and enforcement activities as appropriate. All federal, state, and local law enforcement agencies with significant regulatory and enforcement missions, including Customs, Immigration, the Food and Drug Administration, the Environmental Protection Agency, the Bureau of Alcohol, Tobacco, and Firearms, the Drug Enforcement Administration, the FBI, the Coast Guard, and the Departments of Agriculture, Commerce, and Labor, should participate on a joint basis. The Intelligence Community should, to the extent allowed by law, support these threat assessments. Customs should coordinate this initiative, and should consider providing a sanitized version of the crime threat assessment to the private sector.

Finding 6. Certain existing statutes, regulations, and sentencing guidelines do not provide sufficient sanctions to deter criminal or civil violations related to the import and export of goods and contraband, fraud, cargo theft, and other non-drug-related crimes.

Recommendation 6. Promote enactment as soon as possible of the 21st Century Law Enforcement and Public Safety Act, which includes proposals for the creation of new criminal violations and enhanced penalties related to seaport crime. Additionally, federal agencies—including Customs, Commerce, Health and Human Services, Environmental Protection Agency, and others—should work with the Department of Justice to identify needs for new statutes and forfeiture provisions, including stiffer civil and criminal penalties for import- and export-related seaport crime. Justice should take the lead in this initiative.

Finding 7. Coordination among law enforcement agencies at all levels of government is generally good where FBI Joint Terrorism Task Forces are located to coordinate the exchange of information and joint investigations. However, the Joint Terrorism Task Forces did not typically focus on activity in seaports. The extent of coordination (among non-law enforcement agencies and key private sector entities) related to counter-terrorism security measures was inconsistent at the 12 seaports surveyed.

Recommendation 7. Intensify the federal government efforts to assist seaports in preparing for the possibility of terrorist acts directed at critical infrastructure. Specifically, the Department of Transportation, as Lead Sector Agency for Transportation in accordance with Presidential Decision Directive 63, should be responsible for coordinating implementation of the following recommendations:

- On an expedited basis, the Coast Guard and the FBI (including the National Infrastructure Protection Center), in coordination with other relevant agencies and the private sector, should develop a system for categorizing seaport physical and information infrastructure based on both vulnerability and threat (e.g., low, medium, and high risk).

The federal government should establish baseline vulnerability and threat assessments for terrorism at U.S. seaports as soon as possible. Priority should be given to the Strategic Seaports, Presidential Decision Directive 40 "Controlled Ports," and economically strategic seaports, the criteria for which should be developed by the Interagency Committee on the Marine Transportation System/Marine Transportation System National Advisory Council. Thereafter, threat and vulnerability assessments should be conducted every three years. The FBI should ensure that seaports are included within its field offices' domestic terrorism surveys to assess the potential threat. The Coast Guard should conduct port vulnerability assessments. Both the FBI and the Coast Guard should coordinate their efforts with other agencies, particularly the Department of Defense for the seaports designated as Strategic Seaports for large-scale military mobilizations, and those designated as Controlled Ports under PDD 40. Results should be made available, as appropriate, to all relevant agencies and local port security committees.

- Coast Guard Captains of the Port and the FBI should ensure that their respective Maritime Counterterrorism Plans and Incident Contingency Plans are updated and coordinated annually, and exercised regularly with other concerned federal, state, local, and private entities.

Finding 8. Passenger processing facilities for cruise ships do not provide the security needed for federal officials to undertake their inspections and related efforts associ-

ated with international travelers and crew members.

Recommendation 8. Develop and propose new regulations to create a secure area (Federal Inspection Stations) in seaports where international passengers or passengers from foreign countries disembark. Customs, Immigration, and other relevant agencies should undertake this initiative on a joint basis.

Finding 9. The continuing increases in international passenger and crew arrivals have placed increasing strains on the current inspection processes of the Immigration and Naturalization Service. With these increases have also come increases in stowaways and alien smuggling.

Recommendation 9. Proceed with the Immigration and Naturalization Service Seaport Reengineering System Pilot Program for managing risk with respect to the admissibility of passengers and crew at the nation's seaports consistent with the President's 2001 budget request.

Finding 10. The federal agency automated systems are not easily accessible from waterfront cargo facilities or remote container examination stations. Lack of ready access impedes service level efficiencies, enforcement activities, and commercial compliance initiatives.

Recommendation 10. Establish, to the maximum extent possible, shared dockside inspection facilities (Federal Inspection Stations) at seaports for use by relevant agencies. Customs should take the lead with this initiative and coordinate it with implementation of the five-year technology plan (see Recommendation 15). Other relevant inspection agencies (e.g., Coast Guard, Food and Drug Administration, Agriculture) should conduct coordinated inspections and staff the Stations appropriately.

Finding 11. Vessel manifest information, import and export, is sometimes deficient for the purposes of import risk assessment and export cargo control. Vessel manifest information is more easily utilized for drug enforcement and commercial compliance efforts if it is received in electronic data formats before the arrival of the vessel.

Recommendation 11. Undertake a comprehensive initiative to improve cargo import procedures and related efforts to target seaport crime. Customs, in consultation with other relevant federal agencies, should:

- Proceed with the development of the Automated Commercial Environment (ACE) and Automated Export System (AES) to ensure the adequacy of underlying Federal automated systems required to process commercial data/information.
- Propose revisions to its regulations to require that all ocean manifests be transmitted electronically to Customs sufficiently in advance of the arrival of the vessel to allow manifest information to be used effectively.
- Propose regulations, and, if necessary, legislation, requiring for all entries, including in-bond entries, the same level of information required for entries released into the commerce of the United States.
- Propose requiring that the above information be transmitted to Customs electronically before release of shipments for movement, including in-bond movement, from the port at which goods covered by the entry first arrive.
- Work closely with all other agencies having enforcement or regulatory responsibilities at the border to arrange for the above information to be distributed on a real-time basis to all agencies having an interest in the goods covered by a particular entry.

Finding 12. Inadequate security, particularly existing cargo control measures, renders U.S. seaports vulnerable to those seeking to acquire or sell U.S. goods illegally.

Recommendation 12. Strengthen the export enforcement programs, while preserving export facilitation, by proceeding as follows:

- The Department of Commerce should engage in rulemaking to require the electronic filing of export documentation for ocean shipping one day before a shipment's departure to facilitate targeting of illegal/illicit shipments and other criminal activity by law enforcement agencies. The proposed rule should provide for waiver authority for exigent circumstances. This information should be made available on a real-time basis to agencies with law enforcement responsibilities related to the seaports.
- The agencies with export enforcement responsibilities should update relevant regulatory authorities to increase fines and penalties (both administrative and civil) for export documentation violations, including provisions for enforcement personnel at all relevant federal agencies to issue on-the-spot fines for export documentation violations.
- All relevant agencies should strengthen government export document review programs aimed at enforcement of export control laws to increase export document review and identification of potential violations, and to increase export control-related investigations and enforcement activity, including legal support.
- Customs and the Office of Export Enforcement in the Department of Commerce should work jointly to improve effectiveness of existing resources by setting appropriate standards for seaports for export documentation compliance checks and by strengthening interagency cooperation.
- Commerce should develop a dedicated team at each Commerce/Export Enforcement field office to work with Customs to target export control crimes and provide training to Customs on export control documentation as needed. Stakeholders, such as freight forwarders, should be targeted for compliance education and outreach by joint Customs and Commerce enforcement teams as needed.

Finding 13. The federal government has established formal structures for coordinating government efforts and developed national strategies to address drug trafficking, terrorism, and other domestic and international crime; military mobilization at seaports; and airport security. Seaport security per se, however, has not been adequately addressed. Stronger and more focused interagency and public/private sector efforts to enhance seaport security are needed to address the threats of crime and terrorism, and to enhance control of imports and exports, in order to meet national security and economic mobility requirements.

Recommendation 13. Create, under the Marine Transportation System initiative, national-level security subcommittees of the Interagency Committee on the Marine Transportation System (made up of representatives from the federal government including Customs, Immigration and Naturalization Service, Maritime Administration, Coast Guard, Federal Bureau of Investigation, and others as appropriate) and the Marine Transportation System National Advisory Council (made up of representatives from the private sector including port authorities, ocean carriers, terminal operators, organized labor, truckers, warehouse proprietors, and railroads) to discuss, evaluate, and propose solutions related to seaport security and to address research and development, with emphasis on emerging technologies.

Finding 14. No minimum security standards or guidelines exist for seaports and their facilities.

Recommendation 14. Develop, through the proposed national-level security subcommittee: (a) voluntary minimum security guidelines for U.S. seaports and their users that are linked to existing Coast Guard Captain of the Port controls of maritime trade; and (b) a model port concept, to include a list of risk-based best practices for use by terminal operators. The voluntary guidelines and the model port concept should take into account the differing risk levels and other security factors among ports and should be reviewed and updated at least every five years. To the extent that this approach does not promote significant and generally uniform security improvements at seaports within the next five years, alternative approaches should be considered, including making such guidelines mandatory. Consistent with Presidential Decision Directive 63, Transportation should be responsible for coordinating implementation, and the security guidelines should address, among other topics, the following:

- Uniform practices for physical security (fences, lighting, gates, etc.); for controlling the delivery, receipt, and movement of cargo, passengers, and crew; and for identifying high-risk individuals who seek access to sensitive areas within the seaport.
- A private sector credentialing process that limits access to sensitive seaport areas. States, unions, port authorities, and/or port terminal operators should administer this process. The national security committee should also assess the desirability and feasibility of utilizing criminal background checks to assist in determining access to restricted or sensitive areas at the seaports, including the advisability of port-specific approaches.
- Restricting the access of vehicles to seaports and facilities in seaports and requiring port authorities and the principal private sector businesses that use seaports to implement procedures that achieve appropriate control and accountability.
- Restricting the carrying of firearms in seaports.
- Developing a private security officer certification program to improve the professionalism of port security officers.

Finding 15. Security-enhancing technology and equipment that could assist law enforcement personnel in accomplishing their missions is not available at most seaports.

Recommendation 15. Develop, on a joint basis with all relevant federal agencies, a five-year crime and security technology deployment plan that addresses examination and investigative technology that can be deployed to seaports. Customs should take the lead in establishing a task force to develop a plan that considers utilizing current mechanisms and programs, such as the Customs Border Integrity Project. This plan should address joint acquisition/use of equipment. Upon completion of the plan, appropriate funding should be sought through the regular budgetary process.

Finding 16. The National Port Readiness Network/local Port Readiness Committee concept in the designated Strategic Seaports is fundamentally sound but in need of increased emphasis.

Recommendation 16. Strengthen, through the National Port Readiness Network, with Transportation and Defense as the lead agencies, the planning and coordination for military mobilization security at each Strategic Seaport. These efforts should include the following:

- Local Port Readiness Committees should actively participate in Department of Defense-sponsored combatant commander and Service mobilization exercises/cargo movements (in addition to their own biennial port readiness tabletop exercises) to ensure realism and efficient use of Department of Defense assets.
- The Department of Defense should assist the Coast Guard in establishing additional security guidelines for commercial facilities handling military cargo at the Strategic Seaports and for those seaports designated as Controlled Ports under Presidential Decision Directive 40.

Finding 17. Seaport security is a complex issue that involves federal, state, and local governments, port authorities, and hundreds of businesses; coordination related to seaport security measures is generally inadequate, in part because security-related meetings are not held in most seaports.

Recommendation 17. Establish local Port Security Committees-or possibly a subcommittee of an existing Harbor Safety Committee or Port Readiness Committee-at seaports, including representatives from the port authority, federal, state, and local governments, and the private sector (including organized labor), to discuss and develop solutions for port-specific security issues. The responsible Coast Guard Captain of the Port should chair the local Port Security Committee.

Finding 18. Information about the movement of vessels, people, and cargo within seaports is not integrated, nor is it always readily available to government and private sector security organizations responsible for detecting, intercepting, and preventing terrorism and other criminal activity.

Recommendation 18. Improve information (including intelligence) collection, integration, and dissemination at seaports by proceeding as follows:

- The Coast Guard should work with relevant agencies to coordinate development of an integrated, real-time information system for tracking the movement of vessels (including cargo and personnel) within the seaport environment. This system would be available for use by relevant law enforcement and inspection agencies in crime prevention and security efforts.
- Law enforcement agencies should develop specific collection requirements for foreign intelligence collection efforts concerning the illicit movement of merchandise and contraband in commercial cargo through seaports.
- The Central Intelligence Agency and other national intelligence agencies should increase foreign intelligence collection efforts aimed at providing specific, actionable information about those international criminal activities affecting seaports that have been identified as national security threats to the United States (e.g., drug trafficking and proliferation of weapons of mass destruction).
- Law enforcement agencies should work together to ensure that they have an effective mechanism to process and share intelligence at the seaport level as appropriate.

Finding 19. The security of foreign seaports has a direct impact on the security of U.S. seaports. Shipping and cargo originating in or transiting foreign ports provide an avenue for the introduction of transnational threats to the United States.

Recommendation 19. Work internationally to strengthen global seaport security by:

- Continuing implementation of the President's International Crime Control Strategy and other related strategies.

- Promoting, through federal agency initiatives and diplomatic channels, the development by cognizant international organizations of appropriate international guidelines for addressing seaport crime and security issues. These organizations include the International Maritime Organization, INTERPOL, the Organization of American States, the World Bank, the International Monetary Fund, and other relevant intergovernmental and nongovernmental organizations.
- Increasing cooperation and information sharing with foreign law enforcement and customs agencies.
- Expanding training in seaport security for less-developed countries that are trading partners. Such training should be targeted toward countries where there are serious problems and/or special law enforcement concerns. Topics should include anti-corruption, export control, and handling of transit goods.

Finding 20. Assessing the adequacy of personnel resources contributing to seaport security is complicated by a combination of many factors. Any such assessment would need to address the following points, among others: (a) all relevant personnel, including criminal investigators, inspectors, analysts and support staff; (b) the interdependency of the federal agency personnel who comprise the "federal team" at seaports; (c) possible application of current and planned approaches to personnel issues associated with air and land ports of entry; and (d) the optimal overall mix of federal/state/ local/private sector personnel and other assets needed to provide an appropriate level of security, including border control, at seaports.

Recommendation 20. Consider initiation, through the new proposed national-level security subcommittee, of a comprehensive, interagency study to analyze the impact of current projections related to seaport crime, trade volumes, technology, and other key factors on future personnel requirements for federal agencies having border control responsibilities at seaports.

Chapter 1: Introduction

On April 27, 1999, President William J. Clinton signed an Executive Memorandum directing the establishment of the Interagency Commission on Crime and Security in U.S. Seaports. The memorandum stated:

> United States seaports are an integral part of our Nation's commerce. Too often, however, they tend to be a major locus of crime, including drug trafficking, cargo theft, and smuggling of contraband and aliens. Moreover, the criminal conspiracies often associated with these crimes can pose threats to the people and critical infrastructures of seaport cities.
>
> Many government agencies at the Federal, State and local level are addressing this significant problem, at times in partnership with the private sector. I have determined that the Nation needs a comprehensive review of the nature and extent of seaport crime and the overall state of security in seaports, as well as the ways in which government at all levels are responding to the problem.

The Executive Memorandum directed that the Commission's report include the following:

- 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.
- Recommendations for improving the response of the federal, state, and local governments to the problem of seaport crime.

A copy of the Executive Memorandum establishing the Interagency Commission on Crime and Security in U.S. Seaports can be found in Appendix A.

The Secretary of the Treasury, the Secretary of Transportation, and the Attorney General were directed to establish the Interagency Commission on Crime and Security in U.S. Seaports. Each appointed a co-chair of the Commission to lead the effort. Fifteen additional Commissioners were appointed from departments and agencies throughout the government that had an interest in seaport crime and security. The Commissioners appointed full-time staff members to carry out the day-to-day work of the Commission.

Related Initiatives About Seaport Security

Throughout this report, the Commission has made regular reference to other related initiatives. After its establishment, the Commission's first step was to review already existing initiatives. The White House, for example, has been active in preparing and implementing national strategies when the issues are critical to the country as a whole and successful response requires the integrated efforts of many agencies. The White House has also published numerous Presidential Decision Directives providing guidance on key issues relevant to seaport crime and security. There is a *National Security Strategy,* an

International Crime Control Strategy, and *The National Drug Control Strategy.* Congress and the President have worked closely in commissioning important studies, including *Critical Foundations—Protecting America's Infrastructure, Aviation and Safety at U.S. Airports, The Maritime Transportation System, International Organized Crime and Cargo Theft,* and the *Ocean Policy Study.* Several other efforts are either ongoing or recently completed.

It is important to understand each of the other efforts and their relationship to the efforts that are the focus of this report. The Commission's study and this report are related to these other efforts in a number of ways. The Commissioners overseeing this report decided that this effort would be consistent with current policy and that it would not duplicate or re-research areas that other study groups had already covered.

A few of the more significant efforts of other groups are summarized in Appendix C.

The Commission's Conceptual Approach

With so much work completed or under way at the national and systems levels, the Commission wanted to take on our established mission by focusing on seaports at the micro-level. We wanted to address issues such as: How do seaports operate? What kind of security is present now and who funds it? What are the roles of the various levels of government? What role does the private sector play? How do seaports prepare for the terrorist threats? How serious is crime at seaports, and what are law enforcement agencies doing about it?

In our research on existing studies and reports, the Commission was unable to find any recent efforts that specifically addressed these questions. In developing our approach, we found that even people who had worked for many years in and around the seaport environment had differing opinions on what constitutes a seaport, what is serious crime, and what should be included in security.

This report defines **seaports** as harbors for seagoing vessels with facilities to lade and unlade cargo and/or passengers and with easy access to the sea (from the 24 nautical mile contiguous zone to the terminal, inclusively). Smaller seaports may simply service vessels. According to the Maritime Administration, there are 361 public seaports in the United States.

Many seaports are small and have limited commerce; only 144 have more than a million tons of cargo. In the larger seaports, the activities can stretch along a coast for many miles, including public roads within their geographic boundaries. The facilities used to support arriving and departing cargo are sometimes miles from the coast. The inland ports accept mostly bulk products such as grain, petroleum, coal, and steel. The seaports that accept international cargo have a higher risk of international crimes such as smuggling of drugs and aliens.

The top 50 ports in the United States account for about 90 percent of all the cargo tonnage. In terms of container shipments, 25 U.S. seaports handle 98 percent of the cargo. Cruise ships visiting foreign destinations embark from 16 ports.

This report defines **crime** as unlawful activity. It can take many forms. For example, there is profit-driven crime, and political-driven crime. There are violent crimes, and there are white-collar crimes. The purpose of this report is to discuss crime as it applies to U.S. seaports, so the report divides its consideration of crime into two forms—terrorism, which generally has political motivations, and all other forms of crime, which are more typically profit-driven.

This report recognizes that seaport crime often has a nexus outside the seaport. In seaports where security is improved, the industry has found that cargo thefts occur after the cargo leaves the seaport. There is a wide variation between examining crimes that occur within the strict confines of a seaport and crimes related to cargo that is imported or exported. And there is a lot of middle ground.

Generally, seaport geographic boundaries are defined. But criminal activity associated with the cargo that comes into the seaport does not always occur on the seaport grounds, or it is not detected until after the cargo leaves the port. Frequently cargo arrives in U.S. ports and the importer files in-bond documents to move that cargo to another city, perhaps thousands of miles away. Technically the cargo is still under federal supervision until importers file their final entry in another location and it is released by Customs.

This report defines **security** as protective measures taken to prevent crime and maintain a state of freedom from danger, harm, or risk of loss to person or property, including measures undertaken by federal border control agencies to interdict goods posing a health or safety threat to the public at large and to prevent the unlawful export of controlled items. Security in this context focuses on the following:

- *Physical security and access control:* measures ensuring that seaport operations and users are protected from unauthorized intrusions into their facilities and systems. Effective physical security and access control in seaports is fundamental to deterring and preventing potential threats to seaport operations, cargo shipments for smuggling or theft, or other cargo crimes. Securing entry points, open storage areas, and warehouses throughout the seaport, controlling the movements of trucks transporting cargo through the port, and searching containers, warehouses, and ships at berth or in the harbor are important requirements. Procedures to identify workers who are arriving, and for deterring and preventing internal conspiracies (when smugglers or other criminal groups have their activities aided by employees in the transportation industry), are also becoming increasingly important.
- *Cargo security:* measures ensuring that cargo is protected from theft or unauthorized access. This includes the physical security measures and procedural security of how information and documentation is controlled and used to facilitate movement of cargo. The integrity of import or export shipments during their transit through seaports is fundamental to ensuring that border control agencies are able to accomplish their mission. Unconstrained by jurisdictional requirements or national borders, criminal organizations are exploiting weak security in seaports and their intermodal connections to commit a wide range of cargo crimes. Levels of containerized cargo volumes are forecast to increase significantly, which will create more opportunities for crime while lowering the statistical risk of detection and interdiction.
- *Passenger and crew security:* protection of persons on board vessels, including protection against terrorist attacks and prevention of unauthorized entry of alien migrants or stowaways. The large numbers of U.S. citizens sailing on international cruises pose a special risk from a security perspective, making it much more akin to the air transport environment. Approximately 80 percent of cruise line passengers are U.S. citizens and 20 percent are aliens. Approximately 92 percent of crewmembers are aliens. The worldwide cruise ship fleet will carry nearly 10 million passengers this year. Cruise ship terminals must be secure to prevent unauthorized people from gaining access to the area. Coast

Guard regulations specify minimum security standards to which cruise ship lines must adhere in order to protect passengers adequately from terrorist attacks.

These Coast Guard regulations apply only to large cruise ships on international voyages. They do not cover ships on domestic voyages (not transiting the high seas), such as sightseeing, gambling, and fishing vessels, nor do they cover commuter and car ferries. Security programs in these sectors are voluntary. Cost considerations often prevent these business sectors from pursuing a solid security program.

- *Military mobilization security:* port readiness measures in the event of war or situations when the federal government requires the use of seaport assets. If U.S. troops and equipment are needed in other parts of the world, they are generally deployed through U.S. commercial seaports. In the event of a contingency, U.S. military and logistical support for overseas operations must now extend greater distances over shorter time lines in order to reach the military theater of operation. Consequently, U.S. seaports have become critical choke points of future military mobilizations. The security of our commercial ports during times of military mobilization ensures that such movements are not disrupted; it is therefore essential to our national defense.

The Seaports Studied and the Commission's Methodology

The Commission surveyed the list of 361 commercial seaports to determine which should be the prime focus of our study.

A select list of some 50 seaports represent 90 percent of all U.S. cargo by tons; 25 of these ports represent 98 percent of the container traffic; and 16 ports represent 98 percent of all international cruise ship passengers. Based on these figures, the Commission deemed it appropriate to limit the scope of on-site surveys. Consequently, the Commission conducted detailed on-site surveys in the following 12 seaports:

Charleston	New Orleans
Detroit	New York/New Jersey
Gulfport	Philadelphia
Long Beach	Port Everglades
Los Angeles	San Juan
Miami	Tacoma

These seaports were selected based on their size and disparate threat level for crime. An effort was made to identify large-, medium-, and smaller-sized seaports with varying levels of threats. An effort was also made to ensure that the full range of seaport activities was covered in the on-site surveys, including cargo processing, bulk and container vessel arrivals, cruise ship operations, and Strategic Seaports used in military operations. In addition to the 12 seaports listed above, the Commission conducted more limited field surveys at Baltimore and Jacksonville. It also made on-site surveys of two major foreign ports—Felixstowe, United Kingdom, and Rotterdam, the Netherlands—to observe "best practices."

- The Commission collected data at each location it surveyed. It toured ocean and land facilities and reviewed security practices. It examined port and terminal facilities, warehouses, and federal inspection stations, along with other port facilities. Many seaport officials were interviewed. The entire methodology and criteria for this collection are provided in Appendix B.

In addition to the focus group interviews conducted during the on-site port surveys, the Commission published a notice in the *Federal Register* to give the private sector an opportunity to comment

in public sessions. These sessions were set in Hampton Roads, Virginia; Houston, Texas; and San Francisco, California. The comments elicited at all of these sessions are detailed in Appendix D. A Web site was established on the Internet to provide information about the study to the general public and to solicit comments from those who could not contact the Commission in person. The Commission also attended conferences of relevant national organizations and solicited comments from many private organizations.

Organization of This Report

The chapters that follow were organized to correspond with the Executive Memorandum that set out the issues to be addressed by the Commission. Chapter 2 addresses the nature of seaports, the various entities operating in a seaport, and the roles of all levels of government. Chapter 3 addresses the nature and extent of crime in seaports. Chapter 4 addresses the terrorist threats; we elected to discuss this issue as a separate topic from other crime because of its importance. Chapter 5 assesses security in seaports and the federal process of examining imported and exported international cargo, passengers, and crewmembers at the seaports. Chapter 6 addresses coordination and cooperation of the diverse levels of government and industry players on the wide array of issues identified in Chapters 3, 4, and 5. Chapter 7 addresses intelligence and information management issues. Chapter 8 discusses international cooperative efforts and best practices in other countries. Chapter 9 summates the evaluation of the Commission's findings and details the main comments and conclusions. Recommendations appear at the end of each chapter where they are discussed in conjunction with findings. Six appendices complement the content of the various chapters.

Chapter 2: Roles and Authorities in Seaports

The 361 U.S. seaports range widely in size and characteristics. Some are multibillion-dollar enterprises. Others just have occasional vessel arrivals. Cargo operations range from container traffic, to liquid bulk such as petroleum, to dry bulk such as grain, to barge traffic carrying iron ore or steel. Some cargo arrives or departs from foreign locations; some travels from one domestic port to another. In this chapter we review the structure of seaports, their regulatory framework, and the interests of their so-called stakeholders. We also discuss the role of the federal agencies that have an interest in seaports, and introduce coordination and cooperation at the seaport level.

Background on seaports. The first seaports in America were built in colonial days, long before there was a U.S. government. The regulatory framework of our nation's seaports evolved very differently from that of other entities such as airports, which were established after the national government was firmly in place.

According to the Maritime Administration, public ports generate significant local and regional economic growth, including job creation. Commercial port activities in 1996 provided employment for 1.4 million Americans. Port activity contributed $74.8 billion to the U.S. gross domestic product, and personal income of $52.7 billion in 1996. Port activities in 1996 accounted for federal taxes of $14.7 billion, and state and local tax revenues amounting to $5.5 billion.

The American Association of Port Authorities reports that direct, indirect, and induced economic impact of the U.S. port industry in 1996 was:

- 13 million jobs.
- $494 billion in personal income.
- $1.5 trillion in business sales.
- $743 billion to the nation's gross domestic product.
- $200 billion in federal, state, and local taxes.

These statistics provide a clear picture of the importance of seaports in the economic well-being of the nation. It is also important to remember that the military now depends on commercial facilities to support its forward presence. Also, the border inspection and control agencies of the federal government view seaports as a cost-efficient place to verify the admissibility of people and goods entering the United States, and to allow departures of regulated commodities.

The Structure and Operation of U.S. Seaports

The structures and operations of seaports vary significantly. States have responsibility for chartering seaports within their territories. These charters generally include specific geographic boundaries. Some are as large as 30 or 40 square miles, including territory that is on the waterfront as well as surrounding areas. Port authorities in the United States are instrumentalities of state or local governments, established by enactment or grants of authority by the state legislature. With respect to port development

and investment, the federal function has historically included construction and maintenance of navigation channels. Shoreside development has been left to the nonfederal public and private sectors.

Public seaport operations. Public seaport agencies in the United States vary widely in structure and operation, not only between states but also within the states themselves. Some are, in fact, "port authorities" in the sense of being autonomous or semiautonomous, self-sustaining public corporations. Others 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, Oregon, Texas, and Washington. Bi-state agencies include the Delaware River Port Authority and the Port Authority of New York and New Jersey.

Port governing boards may be elected or appointed. Some port agencies have the power to levy taxes; others do not. Port authorities are typically empowered to exercise the powers of eminent domain, to conduct studies and develop plans, to levy facility charges, to issue bonds, to sue and be sued, to apply for federal grants, to act as the local sponsor for federal navigation projects, to enter into contracts and agreements, and, frequently, as the Massachusetts Port Authority statute states, "to do all acts and things necessary or convenient to carry out the powers expressly granted in this act." The jurisdiction of most is limited to a single port; some, however, such as the North Carolina and South Carolina state ports authorities, may extend to two or more ports.

The range of port authority activity may also be extended to include airports, bridges, tunnels, commuter rail systems, inland river or shallow draft terminals, industrial parks, foreign trade zones, world trade centers, terminal or shoreline railroads, shipyards, commercial vessels, dredges, marinas, and public recreational facilities. Many port authorities are given police powers, at least to the extent of maintaining security and enforcing board-approved ordinances on properties that they own. A few also exercise regulatory powers, such as licensing stevedores, enforcing local or state environmental and land-use regulations, and managing submerged or tidal lands within the port's jurisdiction.

A recent survey by the American Association of Port Authorities of its U.S. port members identifies 32 "operating," 33 "nonoperating" (or "landlord"), and 9 "limited" operating port agencies. Operating ports are those in which cargo-handling inland from the pier is performed by port authority employees. At landlord ports, these functions are performed by port authority tenants. Limited operating ports combine characteristics of the first two categories, leasing some facilities and operating others.

Private sector operations. Private sector terminal operations are also widespread in virtually every U.S. port. They include private sector tenants of public port agencies, as well as facilities that are both privately owned and privately managed. In addition, many port services, such as railroads, trucking, towage, pilotage, and bunkers, are typically private rather than public sector functions. Many ports, such as Searsport, Maine, and New Haven, Connecticut, are entirely private in the sense that the facilities are all privately owned and have no governing port agency at all.

The beneficiaries, or users, of the seaport are principally the private sector and all those that support seaport operations. The most basic economic activity at seaports is the transportation of merchandise. Importers and exporters, as well as domestic business, use seaports extensively. About 95 percent of the cargo that does not arrive in the United States through contiguous countries travels by ocean. Ocean, rail, and truck carriers all support arriving and departing cargo. Freight forwarders, ware-

houses, customs brokers, and a host of other businesses also support trade.

Cruise ships and other passenger ships such as ferries and gambling ships increase the number of public users of the seaports. This business and all the businesses that support cruise ship operations are expanding dramatically. The number of businesses and suppliers that are required to support a cruise ship of more than 1,500 passengers on a voyage of a week or more is extensive. A cruise vessel the size of the Empire State Building being serviced as if it were a hotel doing all of its cleaning, stocking, checkout, and check-in within 9 to 12 hours creates a very difficult logistic effort for the operators. There is the same impact on the agencies charged with allowing appropriate people and things on and off.

Crews of cruise ships and cargo vessels also arrive regularly at seaports and need service. Those arriving on foreign-owned cruise ships and cargo vessels who are not American citizens require attention from federal officials.

The Federal Role in U.S. Seaports

Unlike many countries, the United States has no national port authority. Instead, jurisdiction over U.S. ports and harbors is shared by the federal, state, and local governments. The Constitution does not establish the regulation of seaports as a federal responsibility, so under the 10th Amendment ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people"), the primary responsibility rests with the states.

The Constitution, however, does grant the federal government jurisdiction over the navigable waters of the United States, including its deep draft channels and harbors—authority delegated primarily to the Coast Guard and the Army Corps of Engineers. Under the Constitution, the federal government also retains jurisdiction over the nation's interstate and foreign commerce. Following from that is the national interest in regulating key operational and functional activities that occur in seaport (i.e., administering tariffs, trade agreements, immigration, prohibited material, and safety of commerce). Thus, there is a significant extent of federal activity in state and privately administered seaports.

Customs Service

The Tariff Act of July 4, 1789 authorized the collection of duties on imported goods. In 1789, the Fifth Act of the First Congress established the Customs Service and its ports of entry. At the time, the Customs mission was to supervise the unlading of vessels, ensure a complete inventory of imported cargo, appraise the value, and collect the applicable duty. For nearly 125 years, Customs duties funded virtually the entire government.

As the nation's principal statutorily established border agency, Customs performs dual missions, one of law enforcement and one of regulating commercial activities. Within its mission, Customs has significant responsibilities 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 mission is based primarily on statutory authority contained in Title 19, Customs Duties, and Title 18, Crimes and Criminal Procedures, of the U.S. Code, which grants statutory and regulatory authority to enforce smuggling laws and to conduct warrantless searches and seizures at the border or the functional equivalent (airports or seaports). Customs also has authority to enforce all violations of U.S. export control laws and economic sanctions and embargoes. In addition, Customs enforces hundreds of provisions contained in more than 600 other laws.

Customs responsibilities include assessing and collecting duties, excise taxes, fees, and penalties due on imported merchandise; ensuring that imports and exports meet legal entry and exit requirements; regulating Customs bonded warehouses and container stations, Customs brokers, bonded carriers, centralized examination stations, and foreign trade zones; processing conveyances, persons, baggage, cargo, and mail; detecting and apprehending persons engaged in smuggling, including illegal drugs, and in fraudulent practices designed to circumvent Customs and related laws; protecting U.S. business, labor, and intellectual property rights by preventing illegal trade practices, including provisions related to quotas and the marking of imported merchandise, and the Anti-Dumping Act; enforcing export restrictions and prohibitions, including the export of strategic dual-use goods and technology and defense articles and services, and economic sanctions and embargoes; and collecting accurate import and export data for compilation of international trade statistics.

The investigative mission of Customs is to identify, disrupt, and dismantle activities of individuals and organizations that are in violation of U.S. laws enforced by Customs. Customs investigative responsibilities encompass a multitude of illegal activities pertaining to the importation and exportation of merchandise and contraband. The majority of the investigations related to seaports are conducted in four major program areas: smuggling, financial, strategic, and fraud. Smuggling investigations may include smuggling drugs and commercial quantities of merchandise, and cargo theft. Financial investigations center on narcotics-related and non-narcotics-related money laundering activities. Strategic investigations may consist of the export of strategic and controlled commodities such as defense articles and services, weapons of mass destruction, dual-use goods and technology, economic sanctions, and stolen property. Fraud investigations may focus on the diversion of in-bond merchandise, textile transshipments, antidumping, intellectual property rights, and public health and safety.

Although states grant authority to establish ports in their geographic areas, in order for a port to receive foreign ships, cargo, and passengers it must be specifically designated as a port of entry by the federal government. This designation places the port under Customs jurisdiction. Implicit in the authority of Customs over border search and inspection and its right to designate ports of entry is the right to maintain a controlled and secure Customs area that facilitates and ensures the integrity of the authorized search and inspection. Not only does Customs have implicit authority to institute a seaport security program to maintain the integrity of the border area, but various provisions in Customs law provide statutory authorization for such a program. Previously existing Customs programs, however, have been eliminated and curtailed through the years as resources were dedicated to growth in priority areas. For example, until the mid-1980s, Customs had a patrol force operating in seaports. It consisted of uniformed officers in marked vehicles, patrolling seaport environs. They were charged with interdiction of contraband and anti-smuggling activities. They usually conducted surveillance of vessels at rest in terminals, and rolling gate checks of dockworkers, crewmembers, visitors, and vendors, as well as trucks and truck drivers. They coordinated their activities with the control force that examined and permitted unlading and release of cargo, as well as the security and local police authorities. This function was eliminated and the resources absorbed into the Customs Service.

Coast Guard

The Revenue Cutter Service, the predecessor to the Coast Guard, was created by an Act of Congress in 1790 to enforce the nation's customs laws on the seas. At that

time, the primary concern was to protect the revenue of the United States by interdicting ships that were attempting to evade Customs officials. Congress has consistently expanded the role of the Coast Guard, so that today it includes maritime law enforcement, marine safety, hazardous cargo control, protection of natural resources, maritime security, national defense, waterway navigational aids, vessel traffic management, and icebreaking.

The Coast Guard's legislated authority for port security began with the Espionage Act of 1917, which gave the Coast Guard that responsibility during times of war. The Magnuson Act of 1950 gave the President authority to "govern the anchorage and movement of any foreign-flag vessels in territorial water, inspect such vessels at any time, safeguard against destruction, loss, or injury from sabotage or other subversive acts, accidents, or other causes of a similar nature, vessels, harbors, ports, and waterfront facilities..." whenever the President found the security of the United States endangered by "war; invasion; potential subversive acts; and/or disturbances of international relations."

Under this authority, President Truman signed Executive Order 10173 in 1950, giving the Coast Guard the authority to prevent both intentional and accidental loss or destruction of vessels and waterfront facilities. The order further directed all agencies and authorities of the U.S. government and state and local authorities to support, conform to, and assist in the enforcement of these regulations. The Ports and Waterways Safety Act of 1972 provided a broad permanent statutory basis for the exercise of nondefense safety and security for protecting vessels, harbors, ports, and waterfront facilities from intentional destruction, loss, or injury due to subversive or terrorist acts. The Coast Guard also has a major responsibility to check and monitor hazardous cargo that is transported by vessel. Hazardous cargo poses a risk to shipping, ports, land transportation, and individuals.

The Coast Guard has the legal authority for enforcing security requirements at all U.S. seaports and waterways. The Coast Guard also has a wide range of legal authority pertaining to its other missions of marine safety, environmental protection, navigational aids, vessel traffic, maritime law enforcement, and national security. Although the Coast Guard does not have an officer physically located at each of the 361 seaports, a Coast Guard "Captain of the Port" structure covers all 361 seaports. The Captain of the Port is usually a senior officer who is also the commanding officer of the Marine Safety Office that covers that geographic area. The Coast Guard's once active port security program (i.e., dedicated headquarters and field unit port security specialists to do contingency planning, conduct vulnerability assessments, and carry out security-related liaison with other agencies) has been curtailed because its resources have been redirected into other mission areas as workloads grew and missions changed.

Immigration and Naturalization Service

At the end of the 18th century, in The Act of March 26, 1790, Congress established a uniform rule for naturalization by setting the residence requirement at two years. This Act represents the first federal activity in an area previously under the control of the individual states. The authority for this Act is an enumerated power in Article 1, Section 8, of the Constitution.

The Act of July 4, 1864, represents the first congressional attempt to centralize control of immigration. Under that Act, a Commissioner of Immigration was appointed by the President to serve under the authority of the Secretary of State.

On March 3, 1891, Congress enacted the first comprehensive law for national control of immigration. The law established the Bureau of Immigration within the Treasury Department to administer all immigration laws. The law further restrict-

ed immigration by adding to the inadmissible classes persons likely to become public charges, persons suffering from contagious disease, felons, persons convicted of crimes or misdemeanors, and aliens assisted by others by payment of passage. Besides its headquarters in Washington, D.C., the Bureau opened 24 inspections stations at land and sea ports-of-entry (including Ellis Island) in January 1892.

In June 1940 the Bureau of Immigration became the Immigration and Naturalization Service and moved to the Department of Justice in a reorganization meant to provide more prevention and correction of illegal immigration. This is an important function of Immigration, because even while the U.S. economy encourages immigration, the overall economy and infrastructure cannot support all who might wish to come to this country.

The Immigration and Nationality Act of June 27, 1952, brought into one comprehensive statute the multiple laws that had governed immigration and naturalization in the United States.

Immigration is responsible for the examination and inspection of all crews and passengers arriving on ships from ports outside the United States. Those found inadmissible may be detained, removed, or deported. Immigration is also responsible for the apprehension of aliens seeking entry outside designated ports-of-entry along the nation's sea boundaries.

The **Department of Agriculture** oversees both import and export cargo transactions through various divisions such as the Animal and Plant Health Inspection Service, Agriculture Marketing Service, and Food Safety and Inspection Service. Agriculture has the second largest presence among the federal inspection agencies represented on the waterfront, and it performs a mission-critical function of protecting both the American consumer and American agriculture (farms, fields, and forests) from harmful pests, diseases, and unfit foodstuffs.

The **Food and Drug Administration** is responsible for a wide bandwidth of product categories that the American consumer comes in contact with. These items can range from the expected (pharmaceuticals) to the surprising (television screens that emit radiation or dinner plates that might contain lead in the glaze) and everything in between that in some manner may come into contact with or be ingested by or expose the American consumer to potential risk if the product were not compliant with the Food and Drug Administration regulations. Although not represented on the waterfront in the same numbers as Customs or Agriculture, the Food and Drug Administration has a vital role in the monitoring of import cargo on the nation's waterfront.

The **Department of Commerce** is responsible for a number of activities affecting U.S. seaports both directly and indirectly. Its Census Bureau is responsible for (among other things) compiling data on imports, exports, and shipping. To meet these data gathering responsibilities, Census is responsible for the shipper's export declaration (SED), one of the principal documents that must be filed with the government. The SED is used for all exports over $2,500. Law enforcement officials use the SEDs to assist in targeting and in investigating export control violations (discussed further in Chapters 3 and 5).

In addition, the Department of Commerce contains the Bureau of Export Administration, which is responsible for issuing licenses for items contained on the Commerce Control List, a list of dual-use items controlled for national security or foreign policy reasons. The export licenses are also key documents that must be available for inspection before shipment of a U.S. export. Export Enforcement, the federal law enforcement agency dedicated solely to preventing and investigating dual-use export control violations, also resides in the Bureau of Export Administration.

Export Enforcement's primary mission is to identify and investigate export control violations before an item can be shipped out of the country. From eight field offices, and as one of several priorities, Export Enforcement is involved in enforcing export controls at the seaports, in conjunction with Customs. It works on an as needed basis with Customs to inspect export licenses and export containers. Enforcement also conducts joint investigations with Customs when the investigation involves a potential export control violation at seaports.

The **Maritime Administration** in the Department of Transportation facilitates the efficient and secure movement of people and cargo in domestic and international waterborne commerce to promote America's economic growth and international competitiveness in a safe and healthy environment. It leads and assists the U.S. maritime industry in achieving and improving competitiveness by ship operators and shipbuilders, improving ports and harbors, fostering an efficient intermodal transportation system, and providing sealift for national security and the national defense. Some of the programs the Maritime Administration is responsible for are the operation of the Merchant Marine Academy; maintenance of the Ready Reserve Force vessels for use during military contingencies and other Department of Defense-sponsored operations; administration of the Maritime Security Program, which provides financial support to U.S.-flag vessels that are committed to meet military requirements during war or national emergency; and administration of a loan guarantee program that provides assistance for construction or reconstruction of vessels as well as shipyard modernization. The Maritime Administration conducts studies on issues relating to shipping and publishes a wealth of data on seaport activities, including a guidebook on port security. The Port and Cargo Security Program aims to reduce criminal exploitation of commercial maritime cargo, particularly drug smuggling, cargo theft, and other forms of cargo crime. Cooperative international seaport security partnerships among government and private sectors is used to facilitate collaboration with multinational entities such as the Organization of American States, the American Association of Port Authorities, the Maritime Security Council and the International Association of Airport and Seaport Police. The program focuses on the Western Hemisphere. The activities are intended to decrease drug smuggling and cargo crimes through commercial maritime conveyances. The Maritime Administration supports improved seaport security measures as a means of constricting access to commercial cargoes by drug smugglers.

The **Department of Defense** also has a major interest in seaports in the event of military mobilization. The Department of Defense, through the Maritime Administration, has port planning orders in place in 13 commercial seaports (designated as Strategic Seaports), which identify tentative arrangements for the use of facilities and services needed for military deployments. Both the Coast Guard and the Maritime Administration work with Defense during times of war.

The **Federal Maritime Commission** is an independent agency that regulates waterborne foreign commerce rates, ensures equal treatment, and protects against unauthorized activity. It also regulates and licenses freight forwarders and consolidators. Its regulatory authority extends beyond U.S. boundaries to foreign companies that do business in international cargo destined for the United States. It is essentially the regulatory agency of the shipping industry. Before 1961, the Maritime Administration and the Federal Maritime Commission were part of the same agency. In 1961 a decision was made to separate the regulatory and the promotional activities of the shipping industry.

The following table summarizes the federal agencies involved or interested in seaport operations.

Federal Agencies That Have an Interest in Seaports

Department of Transportation

Office of Intelligence and Security: Oversees and coordinates the Department's intelligence and security programs and develops long-range plans and policy on domestic and international transportation security matters.

Maritime Administration: Administers programs to aid in the operation of the U.S. flag merchant fleet, supports port and cargo security programs, operates the U.S. Merchant Marine Academy, maintains Ready Reserve Force vessels, and assists military mobilization efforts in the event of war.

Coast Guard: Administers a range of programs, including maritime law enforcement, port safety and security, waterways management, marine environmental response, aids to navigation, and marine inspection and licensing.

Federal Maritime Commission

An independent agency that regulates waterborne commerce of the United States, ensures that U.S. international trade is open to all nations on equitable terms, and protects against unauthorized activity.

Department of the Treasury

Customs Service: Administers 600 laws for 60 agencies to ensure that all goods and persons entering and exiting the United States do so in accordance with all U.S. laws, by inspecting cargo and conducting criminal investigations relating to drug smuggling, fraud, money laundering, and the export of controlled commodities.

Bureau of Alcohol, Tobacco, and Firearms: Enforces laws for alcohol, tobacco, firearms, explosives, and nationwide arson. Its mission is to reduce violent crime, collect revenue, and protect the public through criminal law enforcement, regulatory enforcement, and tax collection.

Internal Revenue Service: Administers the tax code and investigates tax evasion arising from criminal activity, among other things.

Office of Foreign Assets Control: Administers laws, regulations, and economic sanctions and embargoes against "targeted countries" and their nationals, and licenses certain transactions, including importations and exportations, before dealing with "targeted countries" and their nationals.

Department of Justice

Criminal Division: Oversees criminal matters for more than 900 criminal statutes and sets priorities for criminal prosecution.

Federal Bureau of Investigation: Investigates all violations of criminal statutes, unless assigned to another federal agency, with priority to organized crime, drugs, counterterrorism, white-collar crime, and violent crime.

Drug Enforcement Administration: Enforces controlled substances and chemical diversion laws and regulations, and conducts investigations targeting violators at the interstate and international levels.

Immigration and Naturalization Service: Enforces immigration laws, including the inspection of passengers and crew at ports of entry, and the removal, investigation, detainment, or deportation of aliens who have violated immigration or other laws.

Federal Agencies That Have an Interest in Seaports (cont.)

Department of Defense

Joint Chiefs of Staff: The Chairman is the principal military adviser to the President, the Secretary of Defense, and the National Security Council including advice on military mobilization issues such as public seaports readiness for mobilization.

Department of the Navy: In addition to military mobilization issues, the Navy has an extensive maritime intelligence capability that is critical to assessing threats to commercial seaports.

Department of the Army: In addition to military mobilization issues, the Army Corps of Engineers has numerous waterway and port functions, and the National Guard assists with drug interdiction in many seaports.

Transportation Command: Through its transportation component command, the Military Traffic Management Command, operates military ocean terminals; maintains military units at commercial ports in the United States and overseas; and coordinates defense transportation interest in the planning, construction, and maintenance of the national infrastructure of highways, railroads, ports, waterways, aviation facilities, and pipelines.

Department of Agriculture

Animal and Plant Health Inspection Service: Regulates animal and plant health, including prohibiting the entry of dangerous insects and diseases and certifying domestic products for export.

Food Safety Inspection Service: Regulates meat and poultry, including imports, to ensure that they are safe, unadulterated, and properly labeled.

Department of Health and Human Services

Food and Drug Administration: In part through inspecting imports, ensures that food is safe; that human and animal drugs, biological products, and medical devices are safe and effective; and that electronic products that emit radiation are safe.

Centers for Disease Control and Prevention: Administers national programs for the prevention and control of communicable diseases and enforces foreign quarantine activities and regulations.

Department of the Interior

Fish and Wildlife Service: In part through monitoring of imports and exports, conserves, protects, and enhances the habitat of fish and wildlife, including the protection of endangered species.

Department of Commerce

Bureau of the Census: Among other things, compiles statistics on U.S. foreign trade, including data on imports, exports, and shipping.

Bureau of Export Administration: Directs export control policy, including export licensing, and oversees Export Enforcement (see below).

International Trade Administration: Coordinates trade promotion, international commercial policy, market access, and trade law enforcement.

Export Enforcement: Investigates violations of U.S. export control laws relating to dual-use strategic goods and technology and analyzes export intelligence to assess risks of diversion.

Federal Agencies That Have an Interest in Seaports (cont.)

Department of Labor

Fosters, promotes, and improves the welfare of wage earners in the United States. Labor unions such as the longshoremen and the teamsters have significant presence in seaports.

Department of State

Conducts U.S. foreign policy and coordinates international activities of other U.S. government agencies, directs U.S. export control policy of defense articles and services, and oversees the Office of Defense Trade Controls.

Office of Defense Trade Controls: Promulgates the International Traffic in Arms Regulations, which contain the U.S. Munitions List of controlled defense articles and services that require licensing, and issues licenses. Requires persons engaged in the business of exporting defense articles and services to register with the State Department.

National Security Council

Advises and assists the President in integrating all aspects of national security policy as it affects the United States—domestic, foreign, military, intelligence, and economic.

Central Intelligence Agency

Collects, produces, and disseminates foreign intelligence on national security issues, including international drug trafficking, and conducts foreign counterintelligence activities.

Office of National Drug Control Policy

Establishes policies, objectives, and priorities for the national drug control program.

Environmental Protection Agency

Implements federal laws designed to promote human health by protecting the Nation's air, water, and soil from harmful pollution. Coordinates effective action for the environment including monitoring damage done to marine life as a result of the shipping industry.

U.S. Trade Representative

Coordinates trade policy for the United States and negotiates and controls international trade agreements.

Other Federal Agencies

The federal role at U.S. seaports is broad, particularly at seaports designated as ports of entry. Federal agencies have jurisdiction for a large variety of offenses committed at seaports. For example, the Drug Enforcement Administration has jurisdiction over the controlled substances laws and regulations and conducts investigations of violators operating at the interstate and international levels. The Bureau of Alcohol, Tobacco, and Firearms has jurisdiction involving the importation of munitions. The Environmental Protection Agency has jurisdiction involving environmental offenses. The Federal Bureau of Investigation, in addition to being the lead agency in terrorism matters, has jurisdiction in numerous violations that may occur at seaports, including public corruption, organized crime, labor racketeering, interstate transportation of stolen motor vehicles, and theft from interstate shipment and interstate transportation of stolen property.

Seaport Stakeholders and Their Crime and Security Interests

Another way to look at the structure and operations of seaports, and in particular at security issues at seaports, is from the standpoint of all the public and private entities that hold a stake in the seaports. A major part of the Commission's study involved identifying these stakeholders and obtaining testimony and comments from them as a means of understanding how the pieces fit together. What follows is a rundown of the major categories of stakeholders (other than federal agencies) and what we found their interests and concerns to be with respect to security.

State and local governments are the regulators of seaports, as discussed earlier in this chapter. When crime occurs at the seaports, state and local governments have a major role in investigation and prosecution if a state or local law is violated. Sometimes, the state and local governments provide on-site security through law enforcement officers. For example, in the Port of Baltimore, the state police provide on-site security and patrol the area. In Los Angeles, Miami, and Port Everglades, local law enforcement is actively involved in security. In other cases, local law enforcement responds when a crime is committed. The main concern state and local government representatives expressed to the Commission was that the federal government might give them some federal mandate but not the resources they would need to respond.

Public seaport authorities vary significantly in structure and operation, not only between states but also within the states, as discussed earlier in this chapter. It was our view that port authorities would have a significant interest in identifying and addressing security-related concerns within ports because if they did not they might be perceived as fostering environments that allow crime to exist, and an individual port's reputation might suffer as a result. We found that some of the port authorities take an active role in enhancing physical security by installing fences, lights, gatehouses, and other measures. Some ports had made major efforts and spent considerable resources in improving security. Some port authorities have police divisions consisting of sworn law enforcement officers.

Other port authorities did not appear concerned about security issues and seemed to resist spending their resources on security. Some seaports saw their mission as totally economic and were concerned that any expenditure on security would affect their bottom line. Some port officials, especially where the port authority serves as primarily a lessor, believed that terminal operators or carriers should fund any security enhancements.

Many ports do assist the federal government in dealing with crimes such as drug

and alien smuggling. Other port officials said that was totally a federal responsibility and saw no reason to fund security enhancements that might deal with these crime problems.

Some port authorities, particularly those that had worked hard to improve security, favored the idea of government-enforced security standards universal to all ports. They stated that port authorities that take security measures place themselves at a competitive disadvantage vis-à-vis those that ignore security.

Vessel operators, or carriers, are individuals, partnerships, or corporations engaged in the business of transporting goods or persons for hire. They may own the vessels that transport merchandise from port to port, or they may lease a vessel for a voyage or for an extended period. Vessel operators, or carriers, are responsible for the security of cargo and passengers as they are transported from port to port. However, once the vessel docks and unlades its cargo or passengers, the security of the cargo often becomes the responsibility of the port authority, or a terminal operator. Carriers are legally responsible for any losses of cargo. With regard to international cargo, the federal government holds the carriers responsible for numerous requirements and can issue large fines for noncompliance. For example, Customs has the authority to penalize a carrier millions of dollars if unmanifested illegal drugs are found aboard a vessel.

Many carriers that operate in high-risk environments have developed extensive security programs and work cooperatively with law enforcement officials at all levels. Cargo theft has been a major issue for carriers, and they often opined to the Commission that law enforcement officials do not devote sufficient resources to cargo theft. Piracy on the high seas is also an area that concerns carriers, although it is rare off U.S. ports.

Terminal operators can be carriers, independent firms, or port authorities. Frequently the terminal operator within the port will oversee the unlading of the cargo or passengers from the vessel and the movement of the cargo or passengers to a secure area under the terminal operator's control. If passengers are involved, the terminal operator will oversee the transfer of the passengers from the vessel to federal inspection areas (in the case of international voyages) or shoreside facilities (in the case of domestic voyages). If cargo is involved, the terminal operator will oversee the delivery of the cargo that has been unladed from the vessel to facilities such as warehouses, container freight stations, freight forwarders, importers, and railroads within the immediate area. Most terminal operators provide security services, usually from private security firms. Terminal operators seem to recognize the importance of security, but the cost of providing security is a major issue for them.

Trucking companies in most instances move cargo from the port authority's or terminal operator's facility to warehouses or importers' facilities. Trucking companies are usually common carriers that are engaged in the business of transporting goods for hire. Trucking companies can own the vehicles that transport merchandise, lease vehicles, or hire independent drivers (who own their own trucks) to haul cargo within, or through, the port. While the cargo is being transported from the port authority or terminal operator's facility to the facilities described above, the company transporting the cargo is responsible for its security. The American Trucking Associations has taken a strong stand on cargo security. It has even developed its own national database that is responsive to its needs and is shared with law enforcement agencies. It has been working with law enforcement at all levels to increase security. It is often difficult to determine where cargo was stolen and in whose jurisdiction the crime occurred. In legislative

proposals this year, the American Trucking Associations recommended criminal record checks for truck drivers.

The **warehouse or facility operator** is responsible for the security of the cargo once it is transported to a warehouse or a container freight station. While under the custody of the facility operator, the cargo may be subject to a variety of operations such as unpacking containers, manipulation, storage, and repackaging. Once these operations have been completed, the cargo is normally moved from the facility to the owner or importer via a transportation company's conveyances (such as the facility operator's trucks, an independent trucking company, or the cargo owner's trucks). The trucking company moving the cargo is responsible for its security until the owner or importer takes final delivery of the cargo.

Railroads that service ports can be privately owned, or a port authority can operate them. They are primarily responsible for transporting cargo on railcars from outside the port to shoreside facilities, piers, or terminals within seaports (or vice versa). Some ports even have railyards that permit different railroads to service many carriers and terminal operators. The railyards enable railcars and containers transported via rail to be brought adjacent to vessel operations. The responsibility for the security of the cargo carried via rail begins when the railroad receives the cargo from a trucking company or terminal operator, and ends when the railroad releases the cargo to a trucking company or terminal operator at destination. By federal law, railroads have their own sworn law enforcement to assist in security. The railroads have been aggressive in pursuing security issues.

Importers and exporters cause the transport of merchandise through seaports. **Freight forwarders** assemble small shipments from various shippers into larger shipments. Frequently, freight forwarders will send shipments to be assembled or disassembled (depending on whether cargo is being imported or exported) to break-bulk stations (where containers are unpacked and smaller, less-than-full loads of cargo deliveries are made), or container freight stations that service the seaport, before they are shipped out to their final destination.

Cruise line operators are engaged in the business of transporting persons for hire between ports. Their operations in the United States are governed by regulations administered by the Coast Guard. In addition to ensuring the safe passage of their passengers between ports, they must ensure that their operations and procedures conform to Customs and Immigration regulations and that passengers arriving from foreign countries are conveyed to federal agencies. For the most part, cruise ship operators have taken a strong stand on security and have worked cooperatively with the Coast Guard in implementing the spirit and intent of the regulations. Some of the cruise lines that have implemented the most sophisticated security systems believe the standards should be more aggressively enforced and made more stringent. An important issue for them is the cost of implementing security requirements, and the related issue of whether or not a competitor might be relaxing security to reduce its operating costs.

Contract security plays a significant role in most ports. Most ports do not have dedicated security forces (public or private) that oversee security for the port and for the entities in the port. Instead, most port authorities, carriers, terminal operators, cruise line operators, trucking companies, and facility operators rely upon contact security personnel to provide security at gates, cargo receipt and delivery areas, passenger embarkation and debarkation areas, and other sensitive areas. The personnel who perform security work for contractors may or may not receive security-related training. Some security providers

stated that they were not permitted to supply enough personnel to cover security needs adequately because of the costs.

Labor groups and dockworkers are also significant stakeholders within U.S. seaports. Organized labor performs the lading and unlading of cargo at many U.S. seaports, and performs tasks related to the movement of goods within ports. The Commission received extensive comments from the various labor groups. Some feared for their personal security in seaports and said that security efforts needed to be increased to protect labor. On the West Coast, the longshoremen's union had recently negotiated an agreement with port authorities for the union to provide security. There are variances in how the exclusive bargaining units view access controls being applied to their members. Wearing identification cards and being subject to criminal history checks are opposed by some, while others are more amenable to such controls when equitably exercised.

Trade associations represent carriers, importers/exporters, insurance companies, and others who have an interest in reducing the vulnerability of their members.

Coordination and Cooperation in U.S. Seaports

So many thousands of actions arise every day in the seaport environment that it is difficult to generalize about cooperation and coordination. Once a seaport is chartered by the state, is designated a port of entry by the Secretary of the Treasury, and is able to receive foreign vessels, the port authority or owner/operator is empowered to make business decisions about operations. However, the Coast Guard may deny entry to vessels because of safety or security issues. Customs, Immigration, and Agriculture must be notified of incoming vessels from foreign countries and, depending on the nature of the cargo, any of a host of other federal agencies must be notified. Longshoremen, freight forwarders, importers, exporters, brokers, truckers, rail carriers, and other business entities are also notified so that they can respond to the arriving vessels. Tugboats are often involved in channeling vessel arrivals, and various systems for controlling vessel arrivals are set up in each port. In some of the larger ports, the Coast Guard operates vessel traffic services to eliminate vessel collisions and groundings.

A typical scenario describing a container vessel arriving from a foreign port may be instructive on how interrelated all the necessary transactions are. As the vessel approaches the seaport, the first physical contact usually is taking on board the harbor pilot. Often there is support from tugs to move alongside a container berth where crane operators will offlade the cargo containers. A bunker barge may come alongside the vessel to lade fuel.

The vessel is boarded and cleared by Customs, Immigration, and Agriculture. More frequently, Customs and Agriculture do not go aboard but perform these formalities remotely, or in a central administrative office. Immigration generally goes aboard to muster the crew. Any inspector for a federal agency is dispatched from an administrative office away from the waterfront terminal. Longshoremen go aboard and prepare vessel equipment to discharge containers. Chandlers, suppliers, and repair companies provide service to the vessel at the berth. A controlled gate should review all these persons doing business with or visiting the vessel.

As containers are discharged, the immediate transfer loads are placed directly on rail cars and a unit train is marshaled and dispatched to the trunk railroad carrier. Containers for local delivery are loaded on wheeled chassis and "spotted" in the yard for pickup. High value cargo containers often go to a single location in the yard.

Local drivers are dispatched to the terminal when the vessel operator sends

notice of arrival to consignees. The stevedore verifies that delivery is authorized to the truck driver by the carrier and that there are no federal holds or instructions. In most cases when there is an identified need for examination, containers of interest to a federal agency are transferred to a local container examination station, and released from there. These stations are private enterprises. Customs establishes requirements, and the local industry importers and brokers and truck drivers can select which one to do business with.

While the vessel is in port, the Coast Guard will board and perform a safety inspection for Safety of Life at Sea requirements, load line standards to determine seaworthiness, and verify compliance with pollution controls. The Coast Guard will also review how hazardous cargo is labeled, stored on the terminal, stowed onboard the vessel, and manifested.

This sort of operational scenario happens more than 200,000 times a year and involves more than 10 million loaded container movements into and out of the United States.

There are two things to note in this narrative: (1) the amount of interplay and communication of information required to execute these transactions quickly and smoothly; and (2) the lack of specific verification of all of these transactions by federal entities that could establish better accountability and security in each instance.

The table below lays out the responsibilities for each of the sectors present.

As the table shows, the private sector and the port authorities share several responsibilities with federal, state, or local government entities. Several other responsibilities rest solely with the federal government. Although organized labor has no

Roles and Responsibilities at U.S. Seaports

	Private sector	Port authority	Local gov't	State gov't	Federal gov't
Protect cargo	X		X		X
Protect facilities	X	X	X		X
Port security	X	X	X	X	X
Marine/environment		X	X	X	X
Secure waterways					X
Prevent crime	X	X	X	X	X
Investigate crime*		X	X	X	X
Prevent terrorism	X	X	X	X	X
Control border					X
Military mobilization**		X			X
Regulate or inspect imports					X
Regulate or inspect exports					X
Regulate interstate trade					X

* port authorities with police departments **strategic ports only

specific responsibilities for these major functions relating to crime and security at seaports, it is a strong and active player at seaports. Because of labor unions' large membership, constant presence on the piers, and integral involvement in many critical activities, a cooperative relationship with labor is important. The Commission found excellent cooperation in some seaports and mistrust or unproductive relationships in others. Coordination and cooperation is more fully discussed in Chapter 6.

Crime

Seaports are an entry point and exit point for people, goods, and waterborne conveyances in international trade. The movement of the cargo is an opportunity to perpetrate the crime, or to be integral to the crime. For federal law enforcement, seaports provide a critical opportunity to detect and interdict illegal flows of contraband, cargo, and persons, through the use of warrantless searches that may be conducted at the border. Also, because the seaports are an important link in the logistical supply chain for goods consumed or products going to international markets, they are important infrastructures for the security of the United States, both militarily and economically.

Because of the wide variety of federal agencies concerned with admissibility of goods, and the wide variety of jurisdictions and control by federal, state, and local entities, there are necessarily a wide variety of responses. These responses make allowances for the different geographical makeup of ports and for the expansive variety of specialization of infrastructure investment—for example, the different equipment required by a petroleum refinery, the wood pulp and forestry export industry, and general cargo on board massive container carriers. These industries all require different landside capabilities and necessarily different applications to similar security needs. All of these factors need to be discussed and decided when the issue of cooperation and coordination on crime prevention and suppression are being addressed. This is because a combination of responses are needed among the federal, state, local, and private sectors. These issues are discussed in Chapter 3.

Terrorism

On terrorism issues, the federal government has the clear lead in coordinating the nation's ongoing response. Clear guidance has been issued to the Executive Branch through Presidential Decision Directives, which assign roles and responsibilities to appropriate federal agencies and set forth policy and procedures. While these federal roles are clear, what is less clear is who at the local seaport level is responsible for specific actions on the preventive side. Positive steps to reduce the vulnerability of seaports to terrorism, and who has the responsibility for action, need to be clearly stated and shared with those responsible. These issues are discussed in Chapter 4.

Security

Seaport security could be considered to be under the purview of the terminal owner/operators. Some take this responsibility more serious than others do. Although security requirements could be directed by the states, they generally have not been.

The federal government has several strong interests in this area. Pursuant to Presidential Decision Directive 63, the Secretary of Transportation has the lead responsibility to coordinate both public and private sector efforts to protect critical infrastructure within the transportation sector, including seaports, against terrorism and other threats. The federal government also plays a role through the National Port Security Committee to control embargoes and monitor vessels of certain foreign states while they are in U.S. waters. The Coast Guard has the lead responsibility among the federal agencies for waterway

safety and security and for waterfront facilities, while Customs and Immigration are concerned about security of passengers, and the Coast Guard and Customs are concerned about international cargo.

Security also serves to prevent crime, and for that reason it should be of interest to all seaport stakeholders. For example, law enforcement officials at all levels could view crime prevention as a way to reduce needs for additional resources. The private sector also has a major interest in reducing losses due to theft: a decrease in crime may make the private sector's operations more profitable.

Unlike some of the other areas covered in this report, security responsibilities are not clearly laid out. In some seaports, there may be an active interest in security and in others there may not be much. Most often, security programs are downplayed because of perceived costs. Neither the federal government nor the state governments have taken the lead in this area. These issues are discussed in Chapter 5.

Findings and Recommendations

Finding 2.a. Notwithstanding the existence of a series of Presidential Decision Directives, as well as various national strategies and other directives with application to security in seaports, there exists a need for a more comprehensive and definitive statement of the specific federal responsibilities in this context. Moreover, this statement should be disseminated broadly, particularly to the local levels at which most security activities and operations are undertaken.

Finding 2.b. Most persons who consider the significance of seaports within the larger community see them as vehicles to promote economic growth. Attention to seaport security is insufficient in part because dissemination to the local levels of what national efforts are underway, and how security can reduce crime and terrorism vulnerabilities, is lacking.

Recommendation 1. Strengthen interagency, intergovernmental, and public/private sector efforts to address the threats of seaport crime (including terrorism), and to enhance control of imports and exports through seaports. Unless otherwise specified in Presidential Decision Directives and other policy documents, lead agencies to initiate action and promote increased cooperation should be as follows: Customs, for international cargo and related contraband smuggling; Immigration, for admissibility of international passengers/crew and alien smuggling; Coast Guard, for seaport security; and FBI, for counterterrorism.

Recommendation 2. Strengthen the efforts of the Marine Transportation System national organizations to enhance the awareness of state and local governments and private sector interests (including labor) of the vital role that seaports play in national security that extends beyond their indispensable contribution to the nation's economy.

Chapter 3: Crime at U.S. Seaports

One of the key objectives of the Commission was to analyze the nature and extent of serious crime in U.S. seaports. No recent studies have addressed crime at seaports in a comprehensive manner. Frequently, news reports point to large seizures of drugs found in shipping containers arriving from foreign countries, or to illegal export of weapons and munitions, or even to cargo that violates intellectual property rights laws. But without a comprehensive view of the nature and extent of crime at seaports, it is difficult to determine the comparative degree of seriousness of the problem.

Method of Data Collection

The Commission's crime data collection effort occurred in two main areas. First, the Commission collected data from all relevant federal agencies for fiscal years 1996 through 1998. Crime data were collected from the Customs Service, the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), the Department of Commerce, the Immigration and Naturalization Service, the Coast Guard, the Bureau of Alcohol, Tobacco, and Firearms (ATF), the Internal Revenue Service (IRS), the Department of Agriculture, the Environmental Protection Agency (EPA), and the Food and Drug Administration (FDA).

Second, the Commission collected crime data from state and local law enforcement agencies for 1996 through 1998, and also conducted on-site studies at the 12 seaports surveyed. More than 200 officials were interviewed from appropriate federal, state, and local law enforcement agencies to discuss their assessment and views of criminal activity, their response to crime, and their recommendations to improve anti-crime efforts at seaports. A number of private sector interests, primarily concerning cargo theft and related issues, were also interviewed.

The Commission collected data on criminal activity relating to the importation of weapons of mass destruction, illegal drugs, currency, firearms and munitions, tainted foodstuffs, pharmaceutical drugs, chlorofluorocarbons, pesticides, child pornography, art and artifacts, endangered species, counterfeit and trademark merchandise, and alien smuggling and stowaways. Information was also collected on cargo theft both in the seaports and in the metropolitan areas, extortion, racketeering, money laundering, bribery, corruption, and environmental crimes relating to Clean Water and Clean Air Act violations. Finally, data were collected on the unlawful export of weapons of mass destruction technology and components, ballistic delivery systems, controlled commodities, firearms and munitions, currency, and stolen vehicles, property, and securities. The type of data collected covered known offenses, arrests, seizures, and recoveries, and information about internal conspiracies. Recognizing the extensive collection, reporting, and analytical programs currently in place to analyze Part I and Part II offenses (defined below) in the Uniform Crime Reporting (UCR) Program, the Commission did not include these offenses in its study of crime at seaports.

Note: Given that terrorism poses a direct threat to our national security, the Commission chose to address this criminal activity as a separate topic in Chapter 4.

Determining the Nature and Extent of Serious Crime at Seaports

In conducting an analysis of the nature and extent of serious crime at seaports, the Commission found that its assessment was dependent on two factors: the availability and collection of crime data by law enforcement agencies and the crime detection capabilities of law enforcement agencies. Both of these factors are discussed below.

Availability and Collection of Seaport Crime Data

The Commission found that the collection of crime data at the seaports was difficult because of five major factors:

1. No nationwide crime data collection and reporting system exists for seaports. For example, the Bureau of Justice Statistics, a component of the Office of Justice Programs in the Department of Justice, is the country's primary source for criminal justice statistics. But none of its programs collect and report crime data by seaports. The UCR Program and the National Incident-Based Reporting System are also nationwide crime data collection and reporting systems, administered by the FBI, but these programs do not collect and report crime data by seaports.
2. Not all law enforcement agencies were able to provide crime data because most federal, state, and local law enforcement agencies do not collect and report crime data by seaports. Many federal law enforcement agencies collect data only by regions, divisions, or districts, which may include metropolitan areas or an entire state or several states, and agencies were unable to extract the data by specific seaports.
3. Many agencies initiate investigations outside of seaports for a number of crimes in which seaports may have been used to facilitate specific criminal activity. But because these investigations are conducted under a number of different case classifications or programs, there is no way to determine with any precision which of them are related to seaports. In addition, criminal activity committed in or facilitated through seaports may be discovered only after the commission of the crime outside of the seaport or in a different city or state. The data from these incidents are nearly impossible to capture and attribute to specific seaports with current law enforcement databases.
4. Inadequate information databases and data collection requirements limit the ability of agencies to collect certain types of information or to capture data specifically by seaports. With the exception of state or local agencies, most agencies do not collect data on the number of "known offenses" committed, and therefore their databases cannot capture this information. (Known offenses were defined as the actual number of offenses based on all reports of criminal activity received from all sources or discovered by officers, regardless of whether anyone is arrested, seizures are made, or prosecution is undertaken.) Known offenses are important because they represent the best depiction of crime and the most meaningful data to determine the actual extent of crime at seaports. Furthermore, certain agencies collect data on seizures, arrests, or investigations by program areas, but these programs are too broad for analysis, and the appropriate data could not be captured by specific seaport.
5. The vast majority of the crime data available from the state and local law enforcement agencies that were responsible for law enforcement at the 12 seaports surveyed related to offenses that were outside the scope of the Commission's study. Agencies at these seaports generally collected and reported only data involving Part I and Part II offenses

in the UCR Program. Part I offenses are homicide, forcible rape, robbery, aggravated assault, burglary, larceny—theft, motor vehicle theft, and arson—the so-called Crime Index. Part II offenses, in which only arrest data are reported, are all other offenses, including other assaults, forgery and counterfeiting, fraud, embezzlement, stolen property, vandalism, weapons, prostitution, sex, drug abuse, gambling, offenses against the family and children, driving under the influence, liquor laws, drunkenness, disorderly conduct, vagrancy, suspicion, curfew and loitering laws, and runaways.

Adequate information databases would have significantly improved our ability to assess the nature and extent of serious crime at seaports. Adequate information databases can also assist in detecting emerging crime trends sooner so that appropriate resource allocations and responses can be made in a more timely manner. Finally, adequate information systems would permit departments and agencies to make rational budgetary and resource decisions based upon empirical data, and could better assist in determining the effectiveness and efficiency of agencies and programs.

Although nationwide strategies such as the International Crime Control Strategy and the National Drug Control Strategy serve to coordinate federal efforts at the national level, there are no comprehensive local strategies or threat assessments at the 12 seaports surveyed. Task forces at the local level to address specific threats have worked well and should continue. But coordination and cooperation would be facilitated if federal, state, and local law enforcement officials had a common understanding of the crime threat.

An annual crime threat assessment at the local seaport level could summarize known criminal activity at the seaport from all law enforcement entities, including all intelligence and other information that can be collected. Through this process, agencies would gain a better understanding of each other's crime problems, thereby enhancing communication, cooperation, and coordination. This could also facilitate joint operations and assist in better allocation of limited resources.

Crime Detection Capabilities of Law Enforcement Agencies

The limited crime detection capabilities of federal law enforcement agencies also hindered the Commission's ability to determine the full extent of crime in seaports.

The ability of agencies to identify and detect criminal activity at seaports is directly related to both resource allocations and agency priorities. Federal agencies can improve coordination among themselves and with state and local governments and the private sector and improve efficiency through information management and increased technology. However, with the tremendous growth in trade and the projections that it will double every decade, and with resource increases not assured, federal agencies make resource allocation decisions based upon agency priorities. Because agencies cannot allocate resources at the same level to address all serious crimes at seaports, they decide which crimes will be addressed proactively and which crimes will be addressed reactively. For example, because of the significant drug smuggling threat at many seaports, substantial portions of Customs resources are devoted to counter the drug threat, while other criminal activities such as commercial smuggling, trade fraud, cargo theft, and the export of drug proceeds and controlled commodities and munitions are allocated fewer resources. Therefore, Customs is in a reactive rather than a proactive posture in addressing certain types of crime, and this affects how well Customs can detect or discover certain crimes that have fewer assigned resources.

In fact, in many locations, for a variety of crimes, we found that Customs criminal

investigators conduct investigations only after they receive substantial information about criminal activity or after inspection personnel detect violations or make seizures. In most cases, the proactive, complex investigations, such as undercover and financial investigations, that are necessary to identify and dismantle criminal organizations operating at or facilitating criminal activity through seaports, are not being conducted. This limitation is important because not all crimes readily come to the attention of law enforcement agencies. The limitation is particularly problematic because the law enforcement officials interviewed and the data collected by the Commission at the 12 seaports surveyed indicate that the most extensive and significant criminal activity involve violations of federal laws. Generally these crimes do not have direct victims reporting offenses or incidents to federal authorities. Therefore, federal agencies must expend a significant amount of time and effort targeting and screening cargo to detect violations and to identify violators. Because resource allocation varies among the different types of criminal activity at seaports, it probably affects how well agencies can detect or discover crimes that have fewer assigned resources. This, in turn, distorts their knowledge of the full extent of those criminal activities, which may ultimately result in the assignment of the limited resources. Federal agencies indicate that without a proactive approach to serious crime, determining the full extent of criminal activity at seaports will be difficult, at best.

The limited amount of contraband technology and surveillance equipment affects the ability of agencies to detect certain criminal activity like drug smuggling, internal conspiracies, cargo theft, and the export of stolen vehicles. Just two of the 12 seaports surveyed had contraband detection technology such as non-intrusive X-ray systems to combat drug smuggling or the export of stolen vehicles, and only one had anticrime equipment, such as surveillance equipment to assist combating internal conspiracies or crewmember drug smuggling.

In the area of export control crimes, which is discussed further in Chapter 5, the minimal level of computer technology to track controlled commodities and the lack of timely and accurate export reporting prevented effective targeting and detection of export crime at seaports.

Full Extent of Serious Crime at Seaports Unknown

As a result of the problems noted above, the Commission believes that the crime data in this report are probably *underreported.* The data, while significant, represent only detected or known criminal activity, and the full extent of crime at seaports is not fully known, but serious crime at seaports is probably more extensive then what is detected, reported, and retrievable from the law enforcement agencies. Most of the agencies could not query their databases for criminal activity at specific seaports. Most attempted to gather their data by manually reviewing files, but not all agencies were able to provide data. The final results are a compilation of database queries and manual file review. This method has limitations in terms of accuracy and completeness, and the resulting statistics should be viewed with these limitations in mind. The data do not provide a complete picture of the crime problem or law enforcement's response to crime, but rather an overview of detected, reported, and retrievable criminal activity.

U.S. Seaports as Major Conduits for Serious Crime

Seaports with international cargo and passengers represent the sea borders of the United States and are increasingly the first and last place that federal authorities are able to exert physical control and authority over international cargo and passengers. Seaports are important "choke points" that make it convenient, efficient, and cost-effective to exercise federal responsibility.

Criminal activity with a nexus to U.S. seaports encompasses a broad range of crimes, including but not limited to the importation of illicit drugs, contraband, and prohibited or restricted merchandise; alien smuggling; trade fraud; bribery; extortion; racketeering; environmental crime; cargo theft; and the unlawful exportation of controlled commodities and munitions, stolen property, currency, and precursor chemicals. Frequently, criminal organizations are well-funded regional, national, and international conspiracies that are as knowledgeable as legitimate traders in their use of the intermodal system, commercial shipping and documentation, and computer technology.

Criminal activity at seaports can generally be viewed in three broad categories.

- The first category involves criminal activity that exploits legitimate international trade or otherwise utilizes the transportation industry in facilitating crime. For example, a drug smuggler may import drugs into the United States concealed in a shipping container aboard a commercial vessel, using a "front company" and without the assistance of industry personnel. This drug smuggling method is commonly referred to as a "consignee load." Another example may be an importer who imports counterfeit merchandise concealed deep inside a shipping container of otherwise legitimate and properly manifested products. An export control example may involve misclassifying or incorrectly describing a riot control vehicle with a pepper spray system as a "truck" in order to export it from the United States without the required export license.
- The second category involves criminal activity committed by smugglers or other organized criminal groups whose criminal activity is aided by corrupt individuals employed in seaports or within the transportation industry. For example, a dockworker employed in a seaport may be paid by a drug smuggling organization to remove shipments of drugs from imported shipping containers. These conspiracies are commonly referred to as "internal conspiracies."
- The third category involves crimes that comprise the Part I and Part II offenses in the UCR Program as noted above. These crimes may be committed against seaport employees, visitors, passengers, crewmembers, and property. These crimes are reported to and pursued by the state or local law enforcement agencies with jurisdictions that include seaports. As noted above, the Commission did not include Part I and Part II offenses in its analysis of the nature and extent of crime in seaports. Nonetheless, the Commission found little evidence that there was a serious problem with these crimes at the 12 seaports surveyed.

The table below depicts broad categories of criminal activity with a nexus to seaports and the government agencies with some degree of jurisdiction. Although the table does not represent a complete list of all criminal activity, it does include the majority of significant criminal activity, which was included in this analysis. The criminal activity in the table is not organized in any particular order of importance or based upon any agency priorities.

Jurisdiction over Criminal Activity at U.S. Seaports

CRIMINAL ACTIVITY	AGENCY
Terrorism	FBI, Coast Guard, Customs, Immigration, Treasury, Bureau of Alcohol, Tobacco, and Firearms, S/L
Crime against shipping, piracy	FBI, Coast Guard, Bureau of Alcohol, Tobacco, and Firearms, S/L
Smuggling (importation) strategic/sensitive: Weapons of mass destruction and components Controlled substances Arms and munitions Monetary Instruments Child pornography Counterfeit U.S. currency Precursor and essential chemicals	Customs, FBI, Drug Enforcement Administration, Bureau of Alcohol, Tobacco, and Firearms, Coast Guard, Secret Service, S/L
Alien smuggling **Unlawful entry** **Stowaways**	Immigration, Coast Guard, FBI
General smuggling (importation): Art and artifacts Endangered species and wildlife Chlorofluorocarbons Prohibited or restricted merchandise Commercial merchandise and alcohol	Customs, FBI, Fish and Wildlife, Environmental Protection Agency, Food and Drug Administration, Bureau of Alcohol, Tobacco, and Firearms, Coast Guard, S/L
Cargo theft: Inside seaport Customs custody Outside seaport Outside customs custody	Customs, FBI, S/L
Cargo control: False manifesting Diversion Substitution	Customs, Food and Drug Administration, Environmental Protection Agency, Drug Enforcement Administration, Agriculture, Commerce
Trade crime: Revenue fraud Intellectual property rights Textile transshipment Antidumping/countervailing duties Child, forced, or indentured labor Trade agreements Country of origin marking	Customs, Commerce, FBI

Jurisdiction over Criminal Activity at U.S. Seaports (cont.)

CRIMINAL ACTIVITY	AGENCY
Other serious criminal activity: Extortion Bribery Racketeering Racketeer influenced and corrupt organizations Money laundering Tax evasion Alcohol and tobacco diversion	FBI, Customs, Drug Enforcement Administration, Internal Revenue Service, Bureau of Alcohol, Tobacco, and Firearms, S/L
Health and safety: Tainted foodstuffs and alcohol Pharmaceutical drugs Insects Dangerous organisms	Customs, Food and Drug Administration, Environmental Protection Agency, Agriculture, FBI, Drug Enforcement Administration, Coast Guard, Fish and Wildlife
Environmental: Hazardous cargo Nonindigenous species Ballast water exchange Deliberate discharge (pollution)	Coast Guard, Environmental Protection Agency, FBI, Customs, Agriculture
Smuggling (exportation) strategic/sensitive: WMD and components Ballistic delivery systems State-of-the-art critical technology Military hardware and equipment Dual-use equipment Monetary instruments Arms and munitions Precursor and essential chemicals	Customs, Commerce, State, Drug Enforcement Administration, Bureau of Alcohol, Tobacco, and Firearms, FBI, Coast Guard, Internal Revenue Service
Smuggling (exportation): Stolen vehicles Stolen property Stolen securities U.S. trade secrets Economic espionage	Customs, FBI, Coast Guard, S/L
Economic sanctions and embargoes: Trading with the Enemy Act; Other	Customs, Treasury, Commerce
Bribery (government officials)	The official's agency, FBI
Assault on federal officer	The officer's agency, FBI

As the table indicates, there are a variety of federal and state and local (S/L) law enforcement agencies with joint jurisdiction depending on the crime.

From the law enforcement officials interviewed and the data collected, the Commission found that the primary criminal activity occurring at the 12 seaports surveyed is violations of federal laws, not violations of state or local laws. Much of it is directly related to the importation and exportation of goods and contraband. International criminal organizations and individuals exploit the tremendous volume of international trade transported through U.S. seaports. Federal agencies are primarily responsible for contraband and alien interdiction, regulating the importation and exportation of cargo, vessels and international passengers, and other border control issues. Most of the state and local law enforcement agencies support federal government anti-smuggling efforts, but focus primarily on violent and property crimes committed on seaport property, and to some extent on security of the seaports. Some seaports with dedicated law enforcement agencies are more proactive with respect to certain types of crimes, such as the export of stolen vehicles or cargo theft, but generally consider most of the criminal activity related to the importation and exportation of goods to be the responsibility of the federal government.

Although the type of criminal activity varies among seaports and regions, the Commission found that drug smuggling was the most prevalent and reported crime problem at the 12 seaports surveyed. However, trade fraud and intellectual property rights violations, stowaways and alien smuggling, cargo theft, the smuggling of chlorofluorocarbons, and the unlawful export of controlled commodities and munitions, stolen vehicles, and currency were consistently problems too. Criminal activity occurs at most of the 12 seaports the Commission surveyed and was not limited to a few specific seaports. Federal agencies stress that criminal organizations, particularly drug smuggling organizations, are extremely resilient and mobile, and will shift their modes and methods and entire smuggling operations within a seaport or to different seaports after law enforcement efforts are intensified in any particular seaport. For example, they may shift their drug smuggling from commercial cargo shipments to crewmember or to passenger ships, or to an entirely different seaport.

Drug Smuggling Most Prevalent and Reported Crime Problem

Drug smuggling is a problem at a number of the seaports the Commission surveyed. Cocaine is the principal illicit drug smuggled into the United States through seaports, but significant quantities of marijuana are also smuggled, according to seizure data. The bulk of illicit drugs enter through commercial traffic, particularly in containerized shipments. Containerized shipments permit drug traffickers to avoid the high fees charged by noncommercial smugglers and insulate smugglers from the drug loads detected by law enforcement authorities. Drugs are also concealed aboard commercial vessels and passenger cruise ships, and are also smuggled by crewmembers and passengers. Drug smuggling by crewmembers is a particular problem at seaports where bulk cargo is imported, according to Customs. Dry or liquid bulk shipments, such as steel, fruits, or oil shipments, by their very nature, are less conducive than containerized cargo shipments to conceal drugs and require smugglers to have more control in order to retrieve the concealed drugs. Therefore, drug smuggling organizations appear to prefer crewmember and vessel concealment methods when bulk vessels are used to facilitate drug smuggling operations at seaports.

Total Narcotics Seizures and Offenses at 12 Seaports Surveyed, FY 1996–1998

Narcotic	Number of Seizures	Weight (in pounds)
Cocaine	429	130,521
Marijuana	752	169,724
Heroin	36	75
	Number of Offenses	**Number of Arrests**
Narcotic Offenses	2,730	959
Internal Conspiracy Offenses	818	219

From fiscal years 1996 through 1998, there were 429 seizures of cocaine totaling 130,521 pounds, 752 seizures of marijuana totaling 169,724 pounds, and 36 seizures of heroin totaling 75 pounds in commercial cargo shipments and vessels and cruise ships reported at the 12 seaports that the Commission surveyed. During this same time period, there were 2,730 narcotic offenses and 959 arrests reported, including 818 internal conspiracy offenses and 219 arrests.

Commercial cargo shipments and vessel drug seizures involved more significant weights, while cruise ship seizures tended to be small amounts and involved less organized smuggling efforts. For example, there were 94 cocaine seizures totaling 437 pounds, 645 marijuana seizures totaling 322 pounds, and 15 heroin seizures totaling 38 pounds reported from cruise ships. Customs indicated that it does monitor cruise ship drug smuggling activity for potential internal conspiracy operations and to determine shifts in smuggling patterns from commercial cargo shipments and vessels.

Narcotics Seizures in Commercial Cargo Shipments and Vessels at 12 Seaports Surveyed, FY 1996–1998

Narcotic	Number of Seizures	Weight (in pounds)
Cocaine	335	130,084
Marijuana	107	169,402
Heroin	21	37

A large portion of the seizures and offenses reported involved commercial cargo shipments and vessels—335 of the seizures of cocaine, totaling 130,084 pounds; 107 of the seizures of marijuana, totaling 169,402 pounds; and 21 heroin seizures, totaling 37 pounds, were reported. Although the total weight of marijuana seized in commercial cargo shipments and vessels was greater than the total weight of cocaine seized, the total amount of marijuana seized trended downward significantly, while the total amount of cocaine seized remained consistent. For marijuana seizures, 105,314 pounds in fiscal year 1996, 34,721 pounds in fiscal year 1997, and 29,367 pounds in fiscal year 1998. For cocaine seizures, 48,067 pounds in fiscal year 1996, 36,852 pounds in fiscal year 1997, and 45,165 pounds in fiscal year 1998. The total weight of heroin seizures also trended downward, from 22 pounds in fiscal year 1996 to 5 pounds in fiscal year 1998.

To put the drug smuggling problem at the 12 seaports in perspective, it is useful to compare these seizures with those made nationally and along the Southwest border during the same period.

Narcotics Seizures in Commercial Cargo Shipments and Vessels, Nationwide, FY 1996–1998

Narcotic	Number of Seizures	Weight (in pounds)
Cocaine	597	188,336
Marijuana	331	304,094
Heroin	32	307

In fiscal years 1996 though 1998, in commercial cargo shipments and vessels at all ports of entry nationwide, there were 597 seizures of cocaine totaling 188,336 pounds, 331 seizures of marijuana totaling 304,094 pounds, and 32 heroin seizures totaling 307 pounds, according to Customs.

Narcotics Seizures in Commercial Cargo Shipments and Vehicles, Southwest Border, FY 1996-1998

Narcotic	Number of Seizures	Weight (in pounds)
Cocaine	26	25,160
Marijuana	149	111,216
Heroin	1	1

In commercial cargo shipments and vehicles at all ports of entry along the Southwest border, there were 26 seizures of cocaine totaling 25,160 pounds, 149 seizures of marijuana totaling 111,216 pounds, and 1 seizure of heroin totaling 1 pound.

Comparison of Narcotics Seizures by Weight in Commercial Cargo Shipments and Vessels at 12 Seaports Surveyed and Southwest Border, FY 1996–1998

Narcotic	12 Seaports (% of lbs. seized nationwide)	Southwest Border (% of lbs. seized nationwide)
Cocaine	69%	13%
Marijuana	55%	36%
Heroin	12%	<1%

The 12 seaports surveyed accounted for 69 percent of all cocaine by weight, 55 percent of all marijuana, and 12 percent of all heroin seized in commercial cargo shipments and vessels at all ports of entry nationwide. In contrast, all of the ports of entry along the Southwest border accounted for 13 percent of all cocaine by weight, 36 percent of all marijuana, and less than 1 percent of all heroin seized in commercial cargo shipments and vehicles nationwide.

Comparison of Number of Narcotics Seizures in Commercial Cargo Shipments and Vessels at 12 Seaports Surveyed and Southwest Border, FY 1996–1998

Narcotic	12 Seaports (% of # of seizures nationwide)	Southwest Border (% of # of seizures nationwide)
Cocaine	56%	4%
Marijuana	32%	45%
Heroin	65%	3%

The 12 seaports surveyed accounted for 56 percent of the number of cocaine seizures, 32 percent of the number of marijuana seizures, and 65 percent of the number of heroin seizures in commercial cargo shipments and vessels at all ports of entry nationwide. In contrast, all of the ports of entry along the Southwest border accounted for 4 percent of the number of cocaine seizures, 45 percent of the number of marijuana seizures, and 3 percent of the number of heroin seizures in commercial cargo shipments and vehicles nationwide.

Drug seizures were reported at 9 of the 12 seaports surveyed (Los Angeles and Long Beach were counted as one seaport), and large amounts of drugs were seized at 8 of the 12. The leaders in drug seizures in commercial cargo and vessels among the 12 seaports were Charleston, Los Angeles/Long Beach, Miami, New Orleans, New York/New Jersey, Philadelphia, Port Everglades, and San Juan. These figures represent only known drug smuggling activity; the full extent of undetected drug smuggling at seaports is unknown.

While significant amounts of narcotics are being smuggled through the seaports, the problem does appear to vary considerably among ports. For pounds of drugs seized from fiscal year 1996 through 1998, the Port of Miami ranked number 1 and Port Everglades ranked number 2 among the 12 seaports the Commission surveyed. During those years, 63,662 pounds of cocaine were seized at the Port of Miami and 30,283 pounds at Port Everglades. Large quantities of cocaine were also seized at Charleston, Los Angeles/Long Beach, New Orleans, New York/New Jersey, Philadelphia, and San Juan. Small quantities of cocaine were seized at Gulfport, and no cocaine was seized at Detroit and Tacoma. Large quantities of marijuana were seized at Los Angeles/Long Beach, Miami, New York/New Jersey, Philadelphia, and Port Everglades. Small quantities of marijuana were seized in Gulfport, New Orleans, and San Juan, and no marijuana was seized at Charleston, Detroit, and Tacoma.

In addition to the severity of the problem, the method of drug smuggling may vary among seaports. For example, in Miami, a large number of drug seizures are made in containerized cargo shipments and vessels, including internal conspiracies and cruise ships, but numerous seizures are also made from vessels on the Miami River. Although part of the Port of Miami, it is not in the strict confines of seaport boundaries. Investigations indicate that the vessel operators involved in drug smuggling are being paid in cocaine by drug trafficking organizations for smuggling drugs into the United States. Illegal drugs are concealed in deep compartments and in fuel and water tanks. In two seizures, nearly 1,500 pounds of cocaine was discovered in welded compartments inside water and fuel tanks and crew quarters, and recently, during a 10-day period, nearly 3,000 pounds of cocaine was seized concealed inside the keels and hulls of four Haitian cargo vessels. It can cost law enforcement authorities between $1,000 and $3,000 to pump out the tanks to search for illegal drugs.

Although there have been significant internal conspiracies reported at New York/New Jersey, consignee loads appeared to be favored by drug smuggling organizations. A seizure of 1,332 pounds of cocaine concealed in commercial paper rolls demonstrates the great lengths to which smugglers go in getting drugs into the country. In this case the smugglers concealed the cocaine deeper within commercial paper rolls after comparing the depth of drill holes made by Customs during an examination of a previous dry run (an empty shipment imported by smugglers to test Customs detection efforts).

Parasitic devices are used to smuggle narcotics aboard commercial vessels. For example, at the Philadelphia seaport 335 pounds of cocaine and 3 pounds of heroin were found concealed in the rudder compartment of an oil tanker while it was at anchorage. Divers, using a small pleasure craft, were involved in removing the narcotics from the vessel once it reached the seaport.

Drug smuggling by crewmembers is a problem at some seaports. For example, in New Orleans, 1,445 pounds of cocaine was seized aboard a vessel arriving from Colombia, and cocaine seizures in the hundreds of pounds are common. In Philadelphia, three crewmembers were arrested for smuggling nearly 15 pounds of heroin into the United States.

Drug smuggling organizations also ship drugs to other countries via the United States. For example, at Charleston 862 pounds of cocaine was seized concealed in five containers of asphalt from Colombia for shipment to Italy. Another container had already been shipped and it was located in Spain and found to contain an additional 160 pounds of cocaine. A controlled delivery to Milan, Italy, was conducted, and Italian authorities arrested three individuals.

Finally, a case in Los Angeles/Long Beach demonstrates that internal conspiracies also operate in foreign seaports—587 pounds of cocaine was seized in nine duffel bags in the tail end of a container from Colombia intended for Vancouver, Canada. After the cocaine was seized, a controlled delivery of the cocaine to Canada was conducted. The investigation by the Royal Canadian Mounted Police revealed an extensive internal conspiracy involving dockworkers at the seaport in Vancouver.

Internal Conspiracies Present Most Serious Challenge to Drug Interdiction Efforts at Seaports

Internal conspiracies were reported at 9 of the 12 seaports surveyed—Charleston, Gulfport, Los Angeles, Miami, New Orleans, New York/New Jersey, Port Everglades, Philadelphia, and San Juan. Again, the full extent of undetected internal conspiracies at seaports is unknown.

Internal conspiracies involve criminal activity committed by smugglers or other organized criminal groups whose criminal activity is aided by corrupt individuals employed in seaports or within the transportation industry. The internal conspiracies detected at the seaports the Commission surveyed were primarily involved with drug trafficking organizations smuggling illicit drugs into the United States. Because the counter-drug effort is a high priority, with more resources allocated to it than are allocated to commercial smuggling or trade fraud, Customs reports that drug smuggling organizations counter these efforts by utilizing internal conspiracies to ensure a safe and dependable method to smuggle drugs into the United States. Customs officials do caution that internal conspiracies may be involved with commercial smuggling, trade fraud, cargo theft, or other criminal activity as well, but to date they have not been detected.

Seaports face several drug smuggling threats, but the most serious challenge to drug interdiction efforts at seaports is the operation of internal conspiracies. Drug trafficking organizations use industry employees to facilitate their drug smuggling operations at seaports. Industry employees include dockworkers, employees of ocean carriers, security firms, freight forwarders, brokers, and other

companies involved in the importation or transportation of goods. Internal conspiracies involve individuals with knowledge of Customs procedures and activity, including methods and patterns of targeting, inspection, examination, surveillance, and investigations. These individuals have unrestricted access at seaports, including vessels, vehicles, piers, warehouses, containers, baggage, passengers, crewmembers, longshoremen, and employees.

Industry employees—although the majority of the individuals prosecuted for their participation in internal conspiracies have been dockworkers and security personnel, others may be involved—may be paid by drug smuggling organizations to remove drugs from containers or vessels at seaports before the containers or vessels can be examined and the drugs detected by Customs. Industry employees may also be paid to provide information about specific imported shipments or details about law enforcement activities and vulnerabilities at seaports.

Internal conspiracies pose the greatest challenge not because of the amount of drugs they import into the United States but because they often utilize the shipments of large-volume, nationally known importers (without the importers' knowledge or participation) to conceal drugs, and Customs is less likely to examine what appears to be legitimate freight. The use of legitimate importers and the ability to remove the drugs before shipments can be examined effectively thwart traditional Customs efforts to target and examine. This may be the most significant vulnerability for Customs. For example, in one case internal conspirators were able to open a container and remove a shipment of cocaine in seven seconds. Without advance information about this smuggling attempt, even if Customs did examine this shipment after the drugs were removed, Customs probably would not detect it as an internal conspiracy.

As discussed in Chapter 5, the increasing pressure to enforce the laws and regulations while rapidly moving containers through seaports has diminished the amount of time Customs has to examine cargo. To carry out its responsibilities in this environment, Customs relies on selective targeting and automation to process imported cargo. In order for this process to be effective, Customs must be assured that the shipments it selects for inspection are intact, undisturbed, and in the same condition as when they arrived in the United States. This is important because Customs physically inspects less than 2 percent of cargo before its released, and therefore all of its inspections must be effective. Selective targeting and automation has generally been effective against consignee drug shipments (those not involving internal conspiracies), primarily because the shipments are intact and undisturbed before Customs inspection. However, no matter how sophisticated or state-of-the-art automated targeting systems become, international shipments will continue to remain vulnerable to internal conspiracies if ocean carriers cannot ensure the integrity of imported shipments.

The components of seaport internal conspiracies include overseas conspirators with access to containers or vessels to conceal drugs, the use of common commodities and importers with unsuspicious importation records, access to containers or vessels in U.S. seaports, knowledge of Customs examination techniques and routines, the ability to remove contraband and reseal containers to maintain the integrity of the smuggling method, and the ability to transport smuggled drugs out of the U.S. seaports without detection.

Internal conspiracies employ numerous methods to smuggle drugs through seaports. Among the common methods is concealment of contraband on vessels or in underwater hull attachments (parasitic devices). Often, duplicate container seals are attached to drug shipments inside the

rear of containers. After removal of the drugs by conspirators, the duplicate is attached to the container, thus concealing the illegal activity from Customs and the ultimate recipient of the cargo. Internal conspirators may load drug shipments in company equipment or in their personal vehicles (some seaports permit employees to park their personal vehicles at dockside) and subsequently depart the seaport with no security screening or accountability. Security guards, shipping office personnel, and security gates may be compromised to facilitate drug smuggling. Deeper concealment inside containers, concealment in the structure of containers, removal of drugs concealed in containers that are in transit to a different seaport after Customs inspection at the first port of arrival, or diversion and removal of suitcases concealing drugs from cruise ships may be employed.

Customs must take steps to ensure that these conspiracies do not remove drugs before it can examine the containers. These steps may include inspecting containers when they are unladed from vessels at dockside or moving them under direct supervision or observation to container enforcement examination stations. Even cargo shipments destined for inspection may have been tampered with before they reached Customs inspection. In many cases Customs must rely on the private sector, including dockworkers (due to labor agreements), to move or unload containers or operate container examination stations, which often are miles away from the seaports, and which themselves are also vulnerable to internal conspiracies. The fact that customhouse brokers know which shipments Customs has selected for examination and when those examinations may take place is a vulnerability.

Internal conspiracies are successful because the individuals involved have unrestricted access and are not subject to security screening and inspection and accountability. Their countersurveillance efforts can defeat law enforcement techniques, and they are easily aware of law enforcement successes. This makes it extremely difficult for law enforcement officers to conduct their work. In some cases, Customs has actually had to remove containers in the middle of the night to shield the examination from individuals involved in internal conspiracies.

Internal Conspiracies and Security at Seaports

Inadequate security does contribute to certain serious crimes at seaports. A relevant example occurred at the Port of Miami, when, during the unloading of a roll-on/roll-off vessel, a van drove onto the vessel's deck. The crane operator moved a shipping container from the top stack of the vessel and placed it on the deck near the van. The driver of a mule (a small truck to move containers around the port) placed a different container on the deck in front of the van to block any dockside view of the activity. Individuals from the van broke the seal on the container and climbed inside the container and removed an estimated 20 to 30 boxes. Ten individuals were involved, and when the third mate confronted the individuals, they threatened his life. The boxes were loaded into the van and it departed. When Customs arrived, no dockworkers were present; only the crewmembers were at the scene. Customs suspects that 1,000 kilograms of contraband was removed and that many of the individuals involved were dockworkers.

This example demonstrates how poor security failed to prevent or even hinder a serious crime in progress. The Port of Miami is located on Dodge Island, which is accessed by one road. The port has a security force and system with physical security and access control measures to control visitors, passengers, seaport personnel, truck drivers, and others, and includes identification cards and criminal records checks for seaport employees with access to restricted

cargo operations. A significant weakness, however, is that dockworkers are permitted to park their personally owned vehicles at dockside or near vessels lading or unlading. Internal conspirators frequently use their personally owned vehicles to remove drugs shipments from the Port of Miami, according to Customs. Moreover, port security personnel do not conduct routine security screening and inspection and accountability of personally owned vehicles or seaport equipment. Effective security screening and inspection of vehicles entering and leaving the seaport in this case probably would have prevented or severely hindered the opportunity to commit this crime. The port security personnel had no records to identify the van or any of the individuals inside that were involved in this crime. Improved accountability would have provided records to identify the vehicle and individuals so that investigators could conduct an appropriate investigation.

An example of the relationship between security and internal conspiracies is two significant internal conspiracy investigations conducted by Customs and DEA at Port Everglades that subsequently resulted in the arrest of 45 individuals, including 35 dockworkers and contract security personnel, on drug smuggling and related offenses. The internal conspirators arrested were well-organized and were knowledgeable of the enforcement activities of the federal agencies, according to Customs. For example, in most seaports, dockworkers move and unlade containers for ocean carriers and Customs, so when Customs needs to move, examine, or unload a container, this work is normally performed by dockworkers. During these cases there were several instances when Customs needed to X-ray a container. The dockworkers involved in the internal conspiracy drove the containers to the X-ray station and to the examination area, where Customs conducted in-depth examinations. This allowed the dockworkers to know exactly what Customs was doing with the containers and permitted them to notify the principal smugglers and other conspirators of the Customs activities. The effect was to effectively defeat the attempts to conduct controlled deliveries of the drug-laded containers to the recipients or to further develop the seizure. During the course of the investigation 6 tons of cocaine and 10 tons of marijuana was seized.

Similar to the Port of Miami, Port Everglades also permitted seaport employees to park their personally owned vehicles near arriving and departing vessels and sensitive cargo operations, and port security did not conduct routine security screening and inspection and accountability of personally owned vehicles or seaport equipment. This was one of the methods most frequently used by the employees involved in the internal conspiracies to remove imported drugs from the seaport, according to Customs. Effective security screening and inspection and accountability of seaport employees and vehicles entering and leaving the seaport probably would have prevented or severely hindered the internal conspirators from removing drug shipments from the seaport in their personal vehicles. Subsequent to these investigations, Port Everglades implemented effective physical, access control, and operational security measures designed to improve security and to specifically counter internal conspiracies.

The combination of the successful investigations noted above and the enhanced security countermeasures are paying off, according to Customs. Port Everglades and the Port of Miami are very similar with respect to their container traffic and countries of origin for imported goods. But the levels of security at the two ports are very different. In fiscal year 1998, Port Everglades' internal conspiracy drug seizures represented 40 percent of its total drug seizures, down from 74 percent in fiscal 1997, and consignee drug seizures have been increasing. In contrast, at the Port of Miami, drug seizures

involving internal conspiracies represented 71 percent in fiscal 1998, up from 45 percent in fiscal 1997.

Another example of the relationship between security and internal conspiracies is an internal conspiracy case at Charleston. After a Customs dockside tailgate examination, a container was ordered to an examination site for further examination. The container was resealed and delivered to the examination site and a locking device was placed on the container, but sometime during that evening dockworkers broke the locking device and removed the container from the examination site. The port authority owns the examination site and uses it to lade and unlade containers. The port authority also allows Customs to use a portion of the building to conduct its examinations at the seaport rather than move containers to a centralized examination station that is off seaport property. The container was found 10 days later in an empty container storage area. When Customs examined the container, the seal had been broken and merchandise had been removed. A hole, tunneled approximately 8 feet into the merchandise, revealed a large void. Not far from this container, a truck driver found several duffel bags containing 291 pounds of cocaine in an empty container. The arrest of an individual and the seizure of cocaine were linked to the 291-pound cocaine seizure. Investigation by Customs, DEA, and the FBI identified a dockworker involved in the drug smuggling conspiracy and resulted in the seizure of 3,086 pounds of cocaine, and 22 arrests, indictments, and convictions, including a dockworker who was responsible for removing the drugs from shipping containers.

Although the examination site was located within the Charleston seaport property, a fence did not protect the examination site where the container was stolen. A fence probably would have prevented the removal of the container by dockworkers. A secure Customs examination station on seaport property would also have prevented the theft of the container. Furthermore, effective security screening and inspection and accountability of seaport employees and vehicles entering and leaving the seaport probably would have prevented or severely hindered the ability of the dockworker to remove drug shipments from the seaport.

Another example of lax security is two significant internal conspiracy investigations conducted by Customs, DEA, and the Waterfront Commission of New York Harbor at New York/New Jersey that resulted in the arrest of 42 individuals, including 13 dockworkers involved in drug smuggling. These investigations resulted in the seizure of approximately 3,100 pounds of cocaine and 35,000 pounds of marijuana. Perhaps more important, however, was that these cases established an extensive alliance between traditional organized crime groups and dockworkers under their control, and Colombian trafficking organizations. The Colombian drug smuggling organizations used corrupt dockworkers to assist in the removal of cocaine from the seaport. In addition, at the time, these investigations revealed a never-before-seen tactic used by internal conspiracies—so-called "Colombian break-in groups"—to remove illegal drugs from waterfront facilities. Dockworkers either located shipping containers or positioned containers near holes in fences protecting terminals or at remote locations inside the terminals for the smugglers. The dockworkers then would advise the Colombian smugglers, who in turn would dispatch Colombian break-in groups to enter the terminal, locate the containers, and remove the drugs. In one case, the group climbed the third tier of a container stack to remove a cocaine shipment. According to Customs, these groups operated in Brooklyn, New York; Port Newark and Elizabeth, New Jersey; Baltimore; Norfolk; San Francisco; and Seattle.

This case clearly demonstrates how inadequate security even failed to prevent outside intruders from entering the seaport and committing a serious crime. Effective physical security and access control measures probably would have prevented or severely hindered these Colombian break-in groups. Repairing downed perimeter fences and holes or breaks in the fencing, proper perimeter lighting, and security screening and inspection and accountability of individuals and vehicles entering and leaving the terminals would have been effective deterrents as well.

An example of how effective security prevented a serious crime is a case involving 806 pounds of cocaine concealed in a container in a warehouse in New Jersey, which was the intended target of a Colombian break-in group. The container had been at a terminal in Staten Island before it was moved to the warehouse. While the container was at a terminal, several individuals were arrested for trespassing by the Port Authority Police Department. The individuals had ladders in their possession to gain access to the terminal and bolt cutters to open containers. At the time of their arrest, they were thought to be cargo thieves, but a subsequent investigation revealed that they were in fact a Colombian break-in group.

These investigations clearly demonstrate the importance of implementing and maintaining effective security measures to prevent unauthorized access to international shipments by internal conspiracies and other criminals.

In spite of the successes in attacking internal conspiracies noted above, the fact remains that internal conspiracies are difficult to detect. Once they are detected it is more difficult to identify the individuals involved, and once the individuals involved are identified it is extremely difficult to gather sufficient evidence for prosecution. Internal conspiracy investigations are tremendously time-consuming and manpower-intensive, and when nonconsensual interceptions are utilized, they may require significant funding for related equipment and expenses. Security countermeasures reduce or eliminate vulnerabilities and opportunities for certain criminal activity. This is particularly applicable with respect to internal conspiracies, crewmember drug smuggling, alien smuggling, and cargo theft. In fact, many law enforcement officials believe that security enhancements are the best long-term measures to combat internal conspiracies. Without enhanced security countermeasures, increasingly more federal, state, and local staffing and resources may be needed to identify, arrest, and prosecute individuals and organizations involved, and other industry employees will continue to be vulnerable to drug smuggling organizations.

Immigration Crime: Stowaways and Alien Smuggling

Stowaways were the largest Immigration problem at 10 of the 12 seaports surveyed. From fiscal 1996 through 1998, Immigration intercepted a total of 1,187 stowaways and 247 individuals with fraudulent documents arriving aboard vessels. Immigration intercepted 108 criminal aliens, another 108 aliens who were found to be smuggling narcotics, and 83 aliens who were smuggled into the United States. Miami and New Orleans reported the largest number of stowaways, 405 and 232, respectively, while Detroit and Tacoma did not report any stowaways.

The impact of stowaways includes disruption of service and direct costs and revenue losses for vessel operators. Stowaways also have posed a physical threat to crew and to the safe operation of ships because of their fear of apprehension.

Immigration Offenses at 12 Seaports Surveyed, FY 1996–1998

Type of Offense	# of Known Offenses
Fraudulent documents intercepted	247
False claims of U.S. citizenship	10
Aliens smuggling narcotics	108
Aliens smuggled into U.S.	83
Cases accepted by U.S. Attorney	30
Stowaways intercepted	1,187
Criminal aliens	108

Another problem that Immigration must deal with is vessel crews. Crewmembers easily obtain visas, and once Immigration processes the arrival of a vessel, the captain is responsible for ensuring that crewmembers without appropriate visas remain on board during the vessel's stay in port. Often the captains do not enforce these restrictions, and no head count or exit inspection of the crew is performed. Immigration does not currently compare the departure manifest with actual departing crew on board at the time of departure. So Immigration has no way of knowing whether manifested crews actually leave on the ship they arrived on, leave on another ship, or remain illegally in the United States.

Smuggling of illegal aliens is also a problem. In the 12 seaports surveyed, from fiscal 1996 through 1998, a total of 83 smuggled aliens were intercepted. However, in the five months beginning fiscal year 2000, 114 smuggled aliens have been intercepted. It is important to realize that the bulk of alien smuggling does not take place within the confines of a seaport of entry, but rather at points contiguous to the port-of-entry.

Maritime smuggling from the Caribbean into South Florida is increasing, and Immigration has recently noticed the reemergence of Chinese boat smuggling on both the East and West Coasts. Immigration arrested 32 illegal aliens in soft-top containers at the Port of Los Angeles. Thirty illegal immigrants from China who crossed the Pacific in specially outfitted cargo containers were arrested at the Ports of Long Beach and Los Angeles. The containers were equipped with food, water, battery-powered lights, portable potties, cell phones, and ladders. Each alien was charged $50,000 by smugglers and had paid $5,000 in advance for the voyage, according to Immigration. Immigration arrested 18 illegal aliens from China after they were found inside a cargo container at the Port of Long Beach. Twelve other illegal aliens from China were arrested after they were found inside a soft-top container at the Port of Seattle. Also, Immigration found three Chinese aliens dead and 15 others in another soft-top cargo container in the Port of Seattle. In addition, and what is most disturbing, is the marked increase over the last several months of Chinese nationals being smuggled into West Coast seaports in hard top containers.

This latest activity is disturbing for two reasons. First, the lives of the illegal aliens are put at serious risk (containers arriving with dead aliens inside are not an uncommon occurrence). Second, finding a container with illegal aliens inside when the containers may be stacked 10 high and 10 across is a daunting, often impossible task.

The current Immigration strategy involves overseas districts and domestic district and sector offices engaging in an integrated enforcement effort across the entire Immigration Service to identify, dismantle, or disrupt alien smuggling organizations. Immigration special agents focus enforcement efforts on targeting complex, sophisticated alien smuggling organizations that are international in scope. These smuggling organizations, based in source countries, in transit countries, or in the United States, may use multiple organizations, or smuggling "subcontractors," to further insulate them from identification and prosecution by law enforcement agencies. Immigration's anti-smuggling strategy

involves all enforcement components of Immigration, and is designed to disrupt alien smuggling activities at all levels of operation. The strategy is crafted to be flexible and seeks the best mix of enforcement responses to changing situations.

Import Crimes Other Than Drugs at Seaports

Except for illicit drugs, this group of import crimes involves numerous types of commodities and goods, but the vast majority of the crimes reported involved trade fraud or commercial smuggling and importations of counterfeit and trademark merchandise.

Trade fraud relates to the protection of revenue and to unfair, predatory trade practices. Trade fraud includes violations involving diversion of imported or in-bond merchandise into the commerce of the United States, textile transshipments, and undervaluation and double invoicing of merchandise, as well as false description of merchandise.

Diversion schemes involve circumventing or manipulating the Customs entry or in-bond systems to avoid paying duty and/or to circumvent trade agreements, import restrictions, intellectual property rights restrictions, and health and safety standards. Textile transshipments involve schemes to illegally import, transport, and transship falsely declared textiles and wearing apparel into the United States to avoid quotas. Undervaluation, double invoicing, or false description of merchandise generally involves schemes to avoid or reduce the amount of duty on merchandise imported into the United States. Intellectual property rights schemes involve the illegal importation, transportation, and distribution of counterfeit goods subject to trademark and copyrights registered with Customs. Public health and safety schemes involve the illegal importation, transportation, and transshipment of items that pose a threat to U.S. consumers and/or the environment, including, but not limited to, tainted or prohibited foodstuffs, medicines, unapproved drugs, and chlorofluorocarbons.

Trade fraud offenses were reported at 9 of the 12 seaports surveyed. At the Ports of Los Angeles and Long Beach, trade fraud is a major problem. From fiscal years 1996 through 1998, these seaports accounted for 98 percent of the nearly $103 million in trade fraud goods seized by Customs. A large number of trade offenses were reported in New York/New Jersey, San Juan, and New Orleans. Most import crimes go

Import Crime Other Than Drugs at 12 Seaports Surveyed, FY 1996–1998

Type of Offense	# of Known Offenses	# of Arrests	# of Seizures	Value of Seizures
Trade fraud	411	90	175	$102,994,627
Counterfeit/trademark	336	58	797	$61,167,785
Child pornography	21	6	8	N/A
Alcohol diversion	17	2	17	0
Precursor chemicals	0	0	0	0
WMD	0	0	0	0
Pesticides	1	0	1	$53,696
Art and artifacts	0	0	0	0
Endangered species	0	0	0	0
FDA-regulated products	7	4	1	$75,000

undetected at seaports because less than 2 percent of the cargo is inspected, according to Customs.

One investigation conducted by Customs in Los Angeles revealed that over a five-year period, 360 shipping containers of wearing apparel and counterfeit Microsoft software were imported into the United States. They were falsely described on import documentation as knockdown furniture headboards. The investigation disclosed that typically the last three rows of the containers were loaded with cartons of headboards and the remainder of the container was loaded with counterfeit software and wearing apparel subject to quota restrictions and high duty rates. The investigation determined that this scheme involved $12 million in counterfeit software and $64 million in wearing apparel. The loss of revenue to the U.S. government was $6.5 million.

In a similar scheme, wearing apparel valued at $80 million, with a loss of revenue to the U.S. government of $7.5 million, was concealed inside 500 containers behind several rows of lawn furniture. The principal had several weeks' advance notice that this investigation had been initiated because the containers were flagged for inspection in the Customs Automated Commercial System. This allowed the principal time to destroy all documentary evidence in the United States before the execution of search warrants and to move his illegal proceeds to offshore locations.

Also related to trade fraud is the illegal importation of counterfeit and trademark material (intellectual property rights). Intellectual property rights offenses were reported at 8 of the 12 seaports surveyed. Intellectual property rights violations were a significant problem in the Ports of Los Angeles and Long Beach. From fiscal years 1996 through 1998, 386 seizures, valued at $28.6 million, came from these two ports. New York/New Jersey reported a large number of seizures, and Miami and Philadelphia reported a large number of intellectual property rights offenses. As a whole, the 12 seaports had 797 seizures, valued at $61.1 million. Nationally for the same period, this type of crime resulted in 7,746 seizures, valued at $198 million. The 12 seaports accounted for 10 percent of the total number of intellectual property rights seizures and 30 percent of the total value of all intellectual property rights seized nationwide.

In a recent investigation, the largest seizure ever of imported counterfeit merchandise, valued at $20 million, occurred in New York. The counterfeit merchandise filled 20 40-foot containers. The importer had evaded Custom's automated targeting four previous times by changing the name of the company.

Cargo Theft Outside Seaports in Metropolitan Areas

The effective operation of the U.S. economy depends, in large part, on the efficient and organized movement of goods between and among all modes (maritime waterways, highways, railways) of the U.S. transportation infrastructure. More than $400 billion is spent annually in the United States on the movement of cargo.

In recognizing that seaports are an important component of the larger transportation system, and that significant portions of international cargo remain under federal custody after departure from seaports, the Commission expanded the scope of crimes in its analysis to include cargo theft in the metropolitan areas.

Cargo theft disrupts the reliable and efficient flow of goods. Cargo theft goes unnoticed by most people outside the transportation industry or the law enforcement community, but it is a serious problem affecting the entire transportation network.

According to the transportation and insurance industry, cargo theft results in

Cargo Theft at 12 Seaports Surveyed, FY 1996–1998

Type of Offense	# of Reported Incidences	# of Arrests	Reported Value of Cargo	Value of Property Recovered
Cargo theft at seaport	138	47	$11,777,984	$2,057,805
Cargo theft in metropolitan area	1153	859	$192,604,983	$100,506,964

heavy costs to industries and consumers. However, the transportation industry as a whole has not been able to provide data indicating the extent and cost of cargo theft nationwide. The American Institute of Marine Underwriters (AIMU) is an association representing more than 100 ocean marine insurance companies. The aggregate premium volume of marine and inland cargo represents about 2 percent and between 5 and 6 percent, respectively, of the total insurance business nationwide, according to the AIMU. The AIMU also could not provide any loss data on the extent of cargo theft nationwide.

The theft of high technology products and components from U.S. manufacturers and their customers could exceed $5 billion annually in direct and indirect costs, according to a study published in 1999 by the Rand Institute. The study estimated that direct losses amounted to $250 million per year and indirect costs, such as lost business, security, and insurance, increased the total in excess of $1 billion. Moreover, the theft of products from the industry's customers could cost another $4 billion.

The law enforcement community has not been able to provide such data. The data cannot be extracted with precision from the Uniform Crime Reporting (UCR) Program because cargo theft is not a specific offense for which data are collected. Cargo theft is not a specific statutory crime (rather, it is larceny, burglary, or robbery depending upon the circumstances); therefore, cargo theft data is included as a larceny-theft, burglary and robbery under the UCR Program. However, inconsistent reporting by law enforcement agencies makes it difficult to retrieve reliable cargo theft data, according to many law enforcement officials. For example, when a container of goods is stolen, it could be recorded as a theft of a motor vehicle, theft from a motor vehicle, or theft of motor vehicle parts or accessories, or even a robbery if force or the threat of force was used during the theft. The value of stolen goods may not be reported at all, when in reality the value of the stolen cargo far exceeds the value of the conveyance.

In addition to the lack of a specific cargo theft offense in the UCR Program, underreporting by the private sector severely hampers the collection of cargo theft data, according to law enforcement authorities. Many cargo theft losses are unreported by the private sector because of high insurance deductibles, rising insurance premiums, self-insurance, fear of negative publicity, between-party settlements, competitiveness within the industry, and their reputation for reliability, according to the AIMU. Law enforcement officials also point out that not only is there underreporting by the private sector, but in many cases when the private sector does report cargo theft incidents, the reports are not timely. This untimely reporting has had a negative impact on the ability of law enforcement authorities to respond and investigate these cargo theft losses. The untimely reporting by the private sector is particularly a problem in cases involving cargo losses

through "leakage" (a term used when the parties are unable to determine the actual point of loss). Many times in cases where disputes are finally resolved, too much time has elapsed for law enforcement agencies to properly investigate those losses. Underreporting of cargo theft not only hinders the collection and analysis of cargo theft data, but may also hinder law enforcement efforts and may limit law enforcement resources that might otherwise be assigned to address cargo theft, according to law enforcement authorities.

Furthermore, the private sector is reluctant to report cargo thefts to Customs in cases where imported goods are still in Customs custody, according to Customs and industry officials. Current law requires Customs to levy penalties on businesses in cases of theft of goods in Customs custody, even in cases where the businesses are not responsible for the thefts. Current law does permit Customs to mitigate the penalties subsequently in cases where business is not responsible, but the law prevents Customs from mitigating the U.S. government duties owed on the stolen imported goods. This disincentive appears to have the unintended consequence of deterring private sector reporting of thefts from Customs custody.

As a result, industry and the law enforcement community have not been able to provide a valid estimate of the severity of the cargo theft problem. Some law enforcement authorities estimate the direct loss of cargo theft to be about $6 billion annually, while many in the transportation industry believe the direct loss exceeds $10 billion annually. The American Trucking Associations estimates the direct loss of cargo theft to be about $6 billion annually, based on its own data collection. Some industry analysts believe the indirect costs, such as lost business and increasing insurance needs, related to cargo theft range from $20 billion to $60 billion each year. If these estimates are close to the actual losses, then cargo theft is indeed a significant problem. This is particularly evident when these estimates are viewed alongside the UCR, which reported that the total value of stolen property in connection with all property crimes exceeded $15.4 billion in 1998. This total includes $3.1 billion for burglary offenses, $4.8 billion for larceny-theft offenses, and $7.5 billion for motor vehicle theft. It is particularly striking, in relation to these figures, that the value of stolen goods in cargo thefts far exceeds the value of the stolen conveyances alone—in this case, $7.5 billion in 1998.

The Commission found that cargo theft is a major concern to the private sector at all 12 seaports surveyed. Most of the cargo theft committed inside the 12 seaports resulted from documentation fraud or leakage. Hijackings or "driver give-ups" (when a truck driver is paid to turn over cargo to thieves) were more common in the metropolitan areas. In fact, the greatest vulnerability in the transportation system appears to be the truck driver, according to law enforcement officials. This is important because 85 percent of all the freight transported in the United States is moved by truck. Drivers are susceptible to hijacking and payments by criminal organizations to give up the cargo and to falsely report the loss as a theft.

Thieves, street gangs, traditional organized crime groups, and emerging organized crime groups all target cargo, but the majority of cargo theft today is committed by organized criminal groups acting with advance information about cargo shipments, according to law enforcement authorities. International organized crime groups could be responsible for nearly half of the estimated $30 billion to $50 billion in cargo stolen worldwide annually, according to some estimates. Former drug traffickers are becoming more involved in cargo theft because of the high profit that can be made and because the criminal sentences are much lower than those for drug offenses, according to law enforcement officials. These individuals and groups are

well-organized and frequently steal goods based upon specific orders placed in advance by "fences," brokers, or others. Thefts occur from warehouses, terminals, truck stops, or any other area where cargo is located. Some organizations are capable of committing cargo thefts that span the jurisdictional boundaries of cities, counties, states, and countries. Once stolen, the goods are quickly disposed of in-state or transported to out-of-state fencing locations or even out of the country. Law enforcement authorities estimate that most stolen goods are disposed of in less than 24 hours. Exported stolen goods may reenter the United States and be sold at a discount, effectively legitimizing illegal profits.

Cargo theft offenses or recoveries were reported at 7 of the 12 seaports surveyed. The largest number of offenses occurred in the metropolitan areas of Los Angeles, Miami, and New York/New Jersey. But the vast majority of the reported thefts take place outside of the seaports in the metropolitan areas. Law enforcement authorities at the 12 seaports, the AIMU, and the study conducted by the Rand Institute all support this finding. Many cargo thefts are committed against trucks coming to and from the seaports, not inside the seaports themselves. Seaports provide central locations where organized crime groups can locate and easily target a wide variety of high-value goods. There were 137 thefts valued at $11.7 million and more than $2 million in recovered property from the seaports in Charleston, Los Angeles/Long Beach, Miami, New Orleans, New York/New Jersey, and Port Everglades. Forty-seven arrests were reported. In contrast, there were 1,153 reported thefts valued at more than $192 million, 859 arrests, and nearly $101 million in recovered property in the metropolitan areas of the Los Angeles, Miami, New Orleans, and Philadelphia.

The Cargo Criminal Apprehension Team (Cargo CATS) was formed by the Los Angeles County Sheriff's Department to address cargo theft in the Los Angeles metropolitan area. The task force consists of state, county, and local law enforcement agencies. The success of Cargo CATS has proven that the surveillance and investigative abilities of a multijurisdictional team exceed those of any single agency. Cargo CATS reported a total of 1,153 grand thefts and robberies valued at $192.6 million, $34.5 million in recovered property, and 238 arrests in the Los Angeles metropolitan area.

The FBI in Los Angeles established a multi-agency Safe Streets Task Force with the California Highway Patrol, the Long Beach Police Department, the Internal Revenue Service, and Immigration to specifically target cargo theft activities in the greater Los Angeles metropolitan area to include the Ports of Los Angeles and Long Beach. This task force recovered more than $2.5 million and made 34 arrests in fiscal years 1997 and 1998. This task force works closely with other Southern California law enforcement agencies and employs sensitive investigative techniques such as undercover operations to address major theft violations.

The Tactical Operations Multi-Agency Cargo Anti-Theft Squad (TOMCATS) was created by the Miami-Dade Police Department to address cargo theft in the Miami metropolitan area. The task force consists of the Miami-Dade Police Department, the FBI, Customs, the Florida Highway Patrol, and the Florida Departments of Law Enforcement and Transportation. TOMCATS reported 393 arrests and recovered property valued at almost $46.5 million. Because there is no formal system to specifically collect cargo theft data, TOMCATS only reports full container recoveries and does not collect data on the number of theft incidents.

New York/New Jersey has fewer than a dozen incidents of cargo theft reported each year, according to the Port Authority Police Department. In contrast, the Water-

front Commission of New York Harbor reported that from fiscal years 1996 through 1998, it received 120 reports of thefts, with a total property value of $9.9 million, and it recovered $2 million in stolen property and made 47 arrests. The difference in reporting probably occurs because the Waterfront Commission requires a quarterly cargo theft report from all businesses that it licenses.

The American Trucking Associations (ATA) created a Cargo Theft Information Processing System (Cargo TIPS) in response to the need for a national cargo theft database. Reports are sent to Cargo TIPS through the Internet or by facsimile. Cargo TIPS has three primary components. The first is the cargo theft reports which provides the core of the database. The second is a method for analyzing and reporting the data. The third is a bulletin board, which permits communication between law enforcement authorities and the transportation industry. Cargo TIPS has 300 contributors. One-third are ATA members and others, and two-thirds are law enforcement agencies. The carriers participating in the Cargo TIPS represent about 50 percent of freight moving by truck in the United States. All state or local law enforcement agencies with cargo theft task forces and the FBI's interstate theft task force units utilize the system, according to the ATA. With the implementation of the Cargo TIPS III in the near future, the public will also be able to access and input data on cargo theft.

Many people in the transportation and insurance industry and in the law enforcement community believe it is essential that any national cargo theft database be managed and operated by law enforcement in order to protect the integrity of the information and the proprietary interests of all the reporting parties. A database managed and operated by law enforcement would ensure the most comprehensive collection and reporting data available nationwide because nearly all state and local law enforcement agencies would report cargo theft data and it would not be restricted to any one mode of transportation.

Some in the transportation industry advocate the creation of a cargo theft offense for the UCR Program. The FBI, which administers the UCR Program and the National Incident-Based Reporting System (NIBRS), does not support adding a cargo theft offense to the UCR Program because the program is in the process of being phased out and eventually will be replaced by NIBRS. A major obstacle to creating a cargo theft category in the UCR Program is establishing a comprehensive definition of cargo theft. Because of the variations in defining similar crimes that occur in different states, it is important that the UCR Program adopt a single definition for each of the chosen offenses to ensure meaningful crime data, according to the FBI. As noted above, cargo thefts can occur from warehouses and other real property and conveyances, and sometimes the use of force may be used. To some extent, these factors influence how a crime is categorized under the UCR Program. Furthermore, separating cargo theft would dilute the almost 70 years of data used for comparison purposes. Another consideration is the major programmatic change that would be required, which would place undue hardship and expense on the cooperative statistical effort of approximately 17,000 city, county, and state law enforcement agencies voluntarily reporting data on crimes.

Instead of using the UCR Program, the FBI supports the use of NIBRS to collect cargo theft data. Cargo theft data can be extracted from NIBRS by querying location and/or cost analysis because most cargo thefts are of higher dollar value than typical larceny-thefts. NIBRS allows for more detailed collection of crime data, to include location of a particular incident, the relationships between victim and offender, and a comprehensive description of the property involved in a larceny-theft or other crime. NIBRS is in fact more comprehensive and provides more detailed

information than the summary data of the UCR Program. While only 10 percent of the nation's population is currently under NIBRS, the percentage is continuing to increase, according to the FBI. NIBRS will permit the collection, analysis, and reporting of data that would enable law enforcement authorities to assess the extent of losses and develop appropriate responses to the problem.

Environmental Crimes at Seaports

Environmental offenses were reported at 8 of the 12 seaports surveyed. Smuggling of chlorofluorocarbons was a problem at a few of the seaports, particularly Miami and Puerto Rico. Chlorofluorocarbons are commonly used as refrigerant in cooling systems, and are known to contribute to the depletion of the ozone layer. In 1996, the United States and other developed nations agreed to phase out chlorofluorocarbon production and to ban most chlorofluorocarbon imports. Since then, a black market has developed in chlorofluorocarbons, which are still legally produced abroad, for use in older machines not adaptable to other coolants. From fiscal years 1996 through 1998, there were 52 chlorofluorocarbon seizures totaling 184,673 pounds at the 12 seaports. Nationwide for the same period, there were 1,651 seizures totaling 579,682 pounds of chlorofluorocarbons. The 12 seaports accounted for nearly 32 percent of the total pounds of chlorofluorocarbons seized nationwide. Miami led the country, with 11 chlorofluorocarbons smuggling cases during this period, but San Juan seized the most pounds of chlorofluorocarbons, 82,896, for the same period. Miami was second, with 52,072 pounds seized, and New York/New Jersey was third, with 45,750 pounds.

In Philadelphia, there have been several cases of chlorofluorocarbons smuggling, including one seizure of 10,000 units of Halon, an ozone-depleting chemical used in fire extinguishers. In San Juan, Customs seized 60,000 pounds of chlorofluorocarbons and arrested and convicted four individuals for smuggling the chlorofluorocarbons concealed in containers of toilet paper and beverages.

The profit margin on smuggled chlorofluorocarbons can approach that of the narcotics trade, according to some law enforcement officials. A 30-pound canister of chlorofluorocarbons can be purchased in Europe for approximately $60 and resold in the U.S. market for $600. One Customs special agent is assigned to target and investigate the importation of chlorofluorocarbons in South Florida. This task is made even more difficult because Customs targeting is predominantly directed toward high-risk drug source countries that are not source countries for chlorofluorocarbons. Thus, one individual's manual targeting effort to pinpoint chlorofluorocarbons importation in Miami has resulted in more chlorofluorocarbons seizures there than anywhere else in the nation. This effort is

Environmental Crime at 12 Seaports Surveyed, FY 1996–1998

Type of Offense	# of Known Offenses	# of Arrests	# of Seizures	# of Pounds Seized
CFCs	27	0	52	184,673
Clean Air Act violations	12	8	0	N/A
Clean Water Act violations	11	0	0	N/A
Other	30	2	3	N/A

not replicated elsewhere, and because this kind of international crime is mobile, violators may shift to other seaports with less intense enforcement efforts. The more chlorofluorocarbons Customs seizes in Miami, the more chlorofluorocarbons may be smuggled through other seaports.

Other serious environmental crimes also occur at the seaports. The Environmental Protection Agency's Criminal Investigation Division (EPA/CID) operates a standing environmental task force encompassing the FBI, the Coast Guard, and all state, local, and federal law enforcement agencies that have jurisdiction at the seaports in South Florida. A recent investigation of a major cruise line is an example of how well this task force has operated. The Coast Guard initially sighted a discharge from one of the cruise line vessels. The task force undertook the investigation, and subsequent cases on the cruise line were opened in Alaska, New York, Miami, Los Angeles, the U.S. Virgin Islands, and Puerto Rico. The investigation resulted in a plea agreement in which the cruise line pleaded guilty to 21 felony counts of dumping waste oil and hazardous chemicals and making false statements and agreed to an $18 million fine, the largest ever to be paid by a cruise line.

Ships that fail to follow the marine environmental standards established by the International Maritime Organization have recently been recognized as a significant source of pollution. Discharges of oil, noxious liquid substances, harmful substances carried in packaged forms, sewage, and garbage are frequently undetected.

In New York, the EPA/CID investigated the dumping of sewage sludge by a barge leasing company. The company has been involved in environmental violations in New York and New Jersey for more than a decade. The company was indicted in New Jersey for 25 felony counts of sewage sludge dumping in New Jersey seaports. More recently, the company purportedly contracted to dispose of sewage at sea properly by using approved practices. In fact, however, it would dump the sludge in New York Harbor and lease the same vessels out to another vendor. Employees of the company were indicted for these criminal violations.

In Puerto Rico, the EPA/CID undertook a successful investigation in partnership with the Coast Guard and the FBI. While a vessel was towing a barge, the towline broke, causing the barge to drift and rupture on a coral reef. The result was the discharge of 750,000 gallons of bunker oil onto the beaches and into San Juan Harbor. The towrope had been repaired only hours before. The corporation was fined $75 million.

Export Crimes at Seaports

Export crimes include the unlawful exportation of controlled commodities such as strategic dual-use goods and technologies (goods and technologies that have both military and commercial applications), defense articles and services, monetary instruments, and stolen vehicles, and violations of economic sanctions and embargoes.

Unlawful Export of Strategic and Controlled Commodities

In furtherance of national security and foreign policy objectives, and to combat international terrorism, the United States controls the export of strategic and sensitive commodities. These items may include sensitive goods and technology, dual-use technologies, defense articles like missiles, munitions, and firearms, weapons of mass destruction material, precursor chemicals for ballistic weapons systems, or chemical and biological material and agents.

Generally, all goods in excess of $2,500 exported from the United States require

shippers to file a shipper's export declaration (SED) at the time the goods are delivered to carriers for lading. Ocean carriers are required to file SEDs and carrier export manifests with Customs up to four days after ships depart the United States. Moreover, the export of specific controlled commodities also requires an approved license from the appropriate department responsible for controlling the specific item to be exported. The Department of Commerce licenses specific items on the Commerce Control List, the Department of State licenses specific items on the U.S. Munitions List, and the Department of the Treasury's Office of Foreign Assets Control (OFAC) administers economic sanctions and regulates certain transactions involving targeted countries or its nationals. Specific controlled commodities require that SEDs be filed with Customs in advance of ship's departure, and exporters and others may be required to obtain OFAC licenses before dealing with a targeted country or its nationals.

SEDs and the carrier export manifests have problems similar to those associated with import manifests. These are described in greater detail in the Chapter 5, but, in short, the vast majority of SEDs and carrier export manifests are extremely vague, lack specific details, and do not provide an accurate inventory of the merchandise onboard vessels. Furthermore, these documents are scrutinized far less frequently than the import documents because of resource allocations, and because they are not required to be filed in advance of export. Without appropriate and detailed information in these documents, filed in a reasonable amount of time in advance of the ship's departure, it is virtually impossible for law enforcement agencies to screen, target, and inspect export cargo. Most of the successful export interdictions have been accomplished through investigations, including undercover operations, and intelligence or information received or developed from sources, according to federal agencies.

These limitations and the resources allocated to export inspections and investigations may weaken U.S. efforts to maintain an effective defense against those seeking sensitive American technology and munitions for the development of weapons of mass destruction or terrorism, and may affect national security interests, particularly U.S. nonproliferation objectives. Furthermore, the illegal export of sensitive technology, munitions, and other controlled items can result in increased risk for U.S. military personnel stationed around the world.

Given the resource allocations targeting the problem, federal agencies are probably detecting only a small portion of the controlled commodities that are being exported illegally. Investigative work by Customs and Export Enforcement in the Department of Commerce indicates that a favored technique among persons unlawfully seeking to export sensitive dual-use

Export Crime at 12 Seaports Surveyed, FY 1996–1998

Type of Offense	# of Known Offenses	# of Arrests	# of Seizures	Value of Seizures
Controlled commodities and munitions	296	26	323	$33,426,794
Currency	33	21	16	$25,085,180
Stolen property	29	10	82	$3,388,675
Stolen vehicles	1732	365	1,861	$48,327,692

goods is to circumvent the export license process by falsifying export license information. Another method is to ship without a license, using a false SED. With considerably less than 1 percent of export cargo inspected at seaports, there are limited obstacles in the way of criminals who unlawfully export controlled items.

Export control violations were reported at 7 of the 12 seaports surveyed. The 12 seaports accounted for 11 percent of the total seizures of controlled commodities and munitions nationwide and 20 percent of the total value. The statistics that are available on export crime between fiscal years 1996 and 1998 show that 296 known offenses and 323 seizures of controlled commodities and munitions were reported. Not surprisingly, because of its high volume of export container cargo, the largest number of reported offenses, 211 out of 296, occurred at Los Angeles/Long Beach. Miami, Port Everglades and Los Angeles/Long Beach also reported a number of seizures. During the same period, export crimes involving controlled commodities and munitions accounted for about 14 percent of reported export offenses—in sharp contrast to stolen vehicles, which are subject to 72-hour advance reporting requirements, and which accounted for about 82 percent.

A joint investigation between Export Enforcement in the Department of Commerce and Customs revealed that a multinational aerospace corporation unlawfully exported more than $3 million in aircraft parts to Iran. The company pleaded guilty and was sentenced to pay a criminal fine of $2.5 million and a civil fine of $500,000. In another joint Office of Export Enforcement/Customs investigation, a shipment of controlled computer equipment destined for Libya, via Cyprus, was detained at the seaport. A Scottish national was subsequently indicted for violations of various export laws. He was found guilty of all charges, was sentenced to 51 months in federal prison, and received a criminal fine of $125,000.

A Customs investigation discovered that a Japanese man purchased 350 handguns and unlawfully exported them to Japan from the seaport in Los Angeles. One of the exported handguns was subsequently used to kill a Japanese police officer. The man who exported the handguns was linked to the group responsible for the sarin gas release in the Tokyo subway system.

In another case, law enforcement officials seized six containers of sodium sulfide, a munitions list item and a component of mustard gas, which were intended for export to the government of Syria. Two additional containers had been shipped before the discovery and were subsequently seized by Italian authorities en route to Syria. The investigation indicated that similar shipments had been exported previously from other seaports.

Unlawful Export of Currency

To facilitate criminal, tax, and regulatory investigations and proceedings, the United States monitors the transportation of currency and monetary instruments through financial reporting requirements. These reporting requirements assist the U.S. government in tracking the movement of crime proceeds, which are used to promote criminal activity; in uncovering the nature, location, source, ownership, and control of criminal proceeds; or in pinpointing avoidance of domestic financial reporting requirements.

Outbound currency seizures were reported at 6 of the 12 seaports surveyed. From fiscal years 1996 through 1998, 2,756 outbound currency seizures valued at $173.5 million were made nationwide, according to Customs. The Southwest border accounted for 590 outbound currency seizures valued at $28.3 million, while the 12 seaports accounted for 16 outbound currency seizures valued at nearly $25.1 million. The Southwest border accounted for 16

percent and the 12 seaports accounted for 14 percent of the total value of outbound currency seized nationwide. While the numbers of outbound currency seizures at seaports are a relatively small portion of the numbers nationwide, the three largest outbound currency seizures ever made by Customs have been in seaports: $11.1 million, $9.5 million, and $7 million.

Drug distribution in the New York metropolitan area brings in between $6 billion and $12 billion annually, according to law enforcement authorities. The exportation of bulk drug proceeds is a serious problem, but resource allocations hamper Customs efforts at targeting outbound currency shipments. In a recent case, more than $11 million was seized in transmission parts being exported to Venezuela. This was the ninth shipment to be exported, and shipments of similar size were exported every six weeks. In a year's time, the drug trafficking organization exported between $50 million and $100 million.

In another case, $895,450 in currency concealed inside acetylene cylinders destined for Cali, Colombia, was seized in Charleston, South Carolina. This shipment originated in Newark, New Jersey.

Export of Stolen Vehicles

Congress has enacted laws to combat the exportation of stolen vehicles. This crime is a particular concern to many American citizens and law enforcement officials; it results not only in the loss of personal vehicles but also in higher insurance rates. In 1998, the FBI Uniform Crime Reports estimated that nearly 1.2 million automobiles valued at $7.5 billion were stolen in the United States. The recovery rate was about 65 percent. According to estimates by the National Insurance Crime Bureau (NICB), of the total number of automobiles stolen in the United States, some 200,000, totaling $4 billion in value, are smuggled out of the country. Fewer than 1 percent of U.S. stolen vehicles smuggled overseas are repatriated.

Exports of stolen vehicles were reported at 10 of the 12 seaports surveyed. Several of the seaports reported significant problems with vehicle smuggling. Miami, Los Angeles/Long Beach, New York/New Jersey, and Port Everglades led the country in this crime, accounting for 1,551 of the recoveries. The 12 seaports accounted for 62 percent of all export recoveries and 66 percent of the total value at all seaports nationwide. Of the 3,018 export recoveries, the 12 seaports accounted for 1,861 export recoveries valued at more than $48 million.

California's Foreign Export and Recovery Team, which was created by state law and consists of the California Highway Patrol, Customs, and the NICB, was formed to combat the export of stolen vehicles from all seaports in the state. The Foreign Export and Recovery Team is funded by surcharges on insurance premiums and vehicle registrations. In the last three fiscal years, this task force recovered 288 stolen vehicles valued at nearly $7 million.

The Miami-Dade County Auto Theft Task Force was formed by the Miami-Dade Police Department, the FBI, Customs, the Florida Highway Patrol, the Florida State Attorney, the Miami City Police Department, the Miami Beach Police Department, NICB, and the Hialeah Gardens Police Department. The task force was created to address the problem of stolen vehicles in the metropolitan area, including the export of stolen vehicles through the port of Miami. In the last three fiscal years, this task force recovered 851 stolen vehicles valued at more than $19 million.

The Miami-Dade Auto Theft Task Force discovered an emerging trend in organized auto thefts. It found that an organization was established as a subgroup of major narcotics operations and South American organized crime groups. The organization's activities were financed with drug pro-

ceeds, and the stolen vehicles were used as partial payment for drugs. (The organization was structured into three tiers. The first level was the financiers and brokers; the second level was the warehousing and shipment of the stolen vehicles; and the third level was the disposition of the vehicles overseas and the financial infrastructure.) The organization rented warehouses, using fraudulent front companies, to receive the stolen vehicles and equipment and to provide a delivery site to receive rented construction equipment, which was also obtained through fraudulent means, and was subsequently stolen too. The warehouse was used to containerize the stolen vehicles and equipment, and then the warehouse was abandoned. The containers were picked up by legitimate shipping companies for export to Venezuela and Colombia. The violators provided the shipping companies with false information for the bills of lading and manifests. In one case, 12 containers were intercepted, resulting in the seizure and recovery of 20 stolen vehicles valued in excess of $850,000. Another 22 high-value stolen vehicles and 20 pieces of stolen off-highway mobile construction equipment valued in excess of $1 million were also recovered.

Stolen vehicles are also a large problem in the New York metropolitan area. Vehicles are being stolen for export to the Dominican Republic, the Middle East, Africa, Russia, and other former Eastern Bloc countries. In one joint New York City Police Department and Customs investigation, 26 persons were arrested, including New York City Department of Sanitation employees. The scheme involved the Sanitation Department's derelict vehicle operation, which administers the removal of junk vehicles on city streets. The arrestees targeted and stole high-value vehicles for theft, and in some cases for export, and the titles and paperwork were tampered with to show that the vehicles were salvaged.

In one undercover operation conducted by the FBI and the New York City Police Department Joint Auto Larceny Task force, 20 convictions were obtained, including that of a corrupt Department of Motor vehicles employee, pursuant to a scheme which involved the re-tagging (tampering with vehicle identification numbers) of hundreds of motor vehicles, many of which were illegally exported to the Dominican Republic via fraudulent certificates of origin for subsequent sale by corrupt car dealerships in Santo Domingo. Retagged vehicles worth $5.5 million were seized in connection with this undercover operation.

Uncovering Other Serious Crime at Seaports

Other serious criminal offenses such as bribery, public corruption, extortion, and racketeering related to seaports are difficult to identify and expose. The extent of these crimes is hard to determine, but most law enforcement officials agree that they do occur at seaports. The most difficult aspect of these offenses is in uncovering the various schemes and the individuals involved because without inside information or sources, it is almost impossible to investigate and prosecute these cases. In some cases, witnesses or victims may be reluctant to come forward and provide the information necessary to initiate an investigation because of the threat of violence or intimidation. In other cases, victims may have committed criminal acts themselves, and coming forward and providing information might subject them to prosecution as well. In still other cases, acts of extortion and racketeering may just be seen as the cost of doing business.

Other serious crime offenses were reported at 5 of the 12 seaports surveyed. From fiscal years 1996 through 1998, a total of 113 offenses involving organized crime activity were reported at these seaports. The primary offense reported was money laundering, which accounted for

98 of the 113 offenses, 102 of the 118 arrests, and all of the seizures reported. The money laundering offenses were primarily related to drug smuggling activities. New Orleans led the 12 seaports, with 82 reported offenses, 63 arrests, and 49 seizures with a value of $3.7 million. In second place was Philadelphia, which reported 7 offenses, 36 arrests, and 11 seizures with a value in excess of $1 million.

Legislative and Regulatory Issues

Many federal prosecutors and agencies, and some private sector stakeholders, advised the Commission that new statutes are needed and that certain existing statutes, regulations, and sentence guidelines are inadequate to deter criminal activity and thus need to be amended.

A number of the recommendations made by federal prosecutors were already included in the Administration's crime bill, the 21st Century Law Enforcement and Public Safety Act. The bill has been introduced in Congress.

Laws should be strengthened to increase the cost of smuggling contraband out of the United States. While there is a general criminal statute for illegal importation activity, there is no equivalent general statute for illegal exports. Our recommendation for a statute for smuggling contraband and other goods from the United States is already included the Administration's proposed 21st Century Law Enforcement and Public Safety Act.

The present criminal sanctions for illegal fraud schemes have not kept pace with the millions of dollars in illegal proceeds made by violators who devise elaborate schemes involving commercial products that endanger the health and safety of Americans and the competitiveness of the U.S. economy. The existing criminal sanctions provide no deterrent value. Therefore, an increase in the penalty from two years to five years for violations of Title 18, United States Code, Section 542 should be enacted. This recommendation, too, is already included in the proposed 21st Century Law Enforcement and Public Safety Act. After the sanctions are increased, a commensurate increase in the sentencing guidelines should also be sought.

The present criminal sanctions for removing goods from Customs custody do not take into account the large sums in illegal proceeds made by cargo theft organizations, nor do they take into account how well these groups are organized or how extensive an impact they have on the American economy. The current sanctions provide no deterrent value.

Existing law requires Customs to levy mandatory fines against carriers and businesses in cases of theft from Customs cus-

Other Serious Crime at 12 U.S. Seaports Surveyed, FY 1996–1998

Type of Offense	# of Known Offenses	# of Arrests	# of Seizures	Value of Seizures
Bribery	2	9	0	0
Public corruption	3	4	0	0
Extortion	1	1	0	0
Money laundering	98	102	63	$4,855,876
Racketeering	4	2	0	0
Tobacco diversion	1	0	1	0
Other	4	0	5	$89,765

tody, even if businesses are not responsible for the thefts. In these cases, Customs may mitigate the fine but not the duty. An unintended consequence is that businesses are reluctant to report these thefts to Customs.

Current sentencing guidelines for violations of intellectual property rights are based on the value of the infringed property and not on the value of lost property. As a result, the current sanctions provide no deterrent value and it is not commensurate with the damage inflicted on copyright and trademark holders.

The present sentencing guidelines for smuggling violations are related to tax or duty loss, and do not adequately address the smuggling of prohibited or nondutiable merchandise. Nor do they address the millions of dollars in illegal proceeds made by violators involved in commercial smuggling activities. The current criminal sanctions provide no substantive deterrent value. The guidelines are not commensurate with the level of illegal proceeds and do not take into account cases where there is no tax loss. Violators view the sentences as minor roadblocks and a cost of doing business. In fact, several violators were back in business shortly after they completed their sentences.

Specific sentencing guidelines for smuggling munitions into the United States must be created. In a case in the Southern District of Florida, a defendant was sentenced under smuggling guidelines for attempting to smuggle surface-to-air missiles into the country. These guidelines are the same as those used for sentencing individuals who smuggle wearing apparel or other goods. Obviously, this level of sentence is inadequate, given the emerging threat of terrorism and especially in cases where individuals may be apprehended before a terrorist act is committed and insufficient evidence exists to prove a terrorism charge, and only a lesser charge of smuggling munitions may be proved.

Penalties for export control violations, including documentation violations, also do not serve as an effective deterrent. Civil penalties can be as little as $10,000 per violation, essentially, the cost of doing business. Failure to present the required documentation on a timely basis may be sanctioned with civil penalties accruing at the rate of $50.00 a day.

Currently, there is no “attempt” provision that would permit the EPA to be proactive in preventing environmental crime and damage. An “attempt” provision would allow for the arrest of individuals before they can take an action that will cause significant harm to the environment. By making an arrest, the EPA can stop someone who is about to commit a crime that puts human health at risk or causes damage to the environment. At present, the EPA can only stop such harmful activity by taking the perpetrator into custody, and that is now possible only after the act is consummated and the damage is done. An “attempt” provision would allow a person who acts alone, and therefore would not be guilty of conspiracy, to be charged. Finally, it would allow prosecution in cases in which business owners and operators walk away from a business location and abandon chemicals on site, leaving to local authorities and to the EPA either to wait for a disaster to occur or to spend money on a cleanup.

At present, when containers intended for export are interdicted with stolen property, such as vehicles, the container or the goods in the container used to conceal the stolen property are not subject to forfeiture. This has created a significant problem in that Customs cannot dispose of the containers or goods used to conceal the stolen property.

A trend may be emerging in counterfeit and trademark schemes. Organizations are lawfully importing products into the United States and then affixing counterfeit or trademark labels on the products and distributing products in the U.S. market. “Works in progress” and instrumentalities,

such as equipment used to finish counterfeit or trademark goods in the United States, are not subject to forfeiture because the goods were not in violation at the time of importation. These products can only be seized as evidence and must be returned after prosecution. This may become a common method used by intellectual property rights traffickers.

Findings and Recommendations

Finding 3.a. U.S. seaports are major conduits for serious crime. A wide range of significant criminal activity is being committed at seaports. Drug smuggling is the most prevalent and reported crime problem, but smuggling of contraband and prohibited or restricted merchandise, stowaways and alien smuggling, trade fraud and commercial smuggling, environmental crimes, and the unlawful exportation of controlled commodities and munitions, stolen property, and drug proceeds are consistent problems too.

Finding 3.b. The primary criminal activity at seaports is violations of federal laws, much of it directly related to the importation and exportation of goods and contraband. Federal agencies are primarily responsible for contraband and alien smuggling, regulating the importation and exportation of cargo, vessels and international passengers, and other border control issues. Most state and local law enforcement agencies support anti-smuggling efforts, but focus primarily on violent and property crimes committed on seaport property. Seaports with dedicated law enforcement agencies are more proactive with respect to certain crimes such as cargo theft and the export of stolen vehicles, but consider most of the import- and export-related crime to be the responsibility of the federal government.

Finding 3.c. Internal conspiracies present the most serious challenge to drug interdiction efforts at seaports because they can thwart traditional Customs Service targeting and examination processes. Drug smuggling organizations use transportation industry employees to facilitate their drug smuggling operations at seaports by controlling and monitoring drug shipments concealed inside cargo shipments of legitimate importers.

Finding 3.d. The Commission was not able to determine the full extent of serious crime at seaports. No national data collection and reporting systems now in place cover serious crime in seaports. Federal agency databases do not adequately collect and report crime data by seaports, and state and local law enforcement agencies do not specifically collect and report crime data by seaports. While significant, the crime data summarized in this report do not reflect the full extent of the problem; serious crime at seaports is probably more extensive than what is detected, reported, and retrievable from federal, state, and local law enforcement agencies.

Finding 3.e. Resource allocations, agency priorities, and contraband detection technology and surveillance equipment affect the crime detection capabilities of federal law enforcement agencies at seaports. Resource allocations are based upon agency priorities, and high priority threats like drug smuggling receive substantial portions of resources, while other crimes such as commercial smuggling and trade fraud receive fewer resources. This affects how well agencies detect these other types of crimes, and without a proactive approach to crime, determining the full extent of criminal activity at seaports is difficult. Only two of the 12 seaports surveyed had contraband detection technology such as non-intrusive X-ray systems, and only one seaport had surveillance equipment. The limited amount of contraband technology and surveillance equipment affects the ability of agencies to detect certain criminal activity like drug smuggling, internal conspiracies, and the export of stolen vehicles.

Finding 3.f. Cargo theft is a major concern to the private sector entities that operate at seaports. Although the vast majority of the reported cargo thefts take place while shipments are outside of the seaports in the metropolitan areas, seaports provide central locations where organized crime groups can locate and easily target a wide variety of high value goods. The lack of a national collection and reporting system for cargo theft data and the underreporting of cargo theft losses by the private sector hinder the assessment of the problem and the development of appropriate solutions.

Finding 3.g. Coordination and cooperation among federal, state, and local law enforcement agencies could be improved at seaports by more joint efforts with a seaport focus. Comprehensive interagency crime threat assessments, which are currently not conducted at seaports, offer one such opportunity. By preparing annual crime threat assessments, federal, state, and local law enforcement agencies would develop a better understanding of the overall crime threat at each seaport and also lay the groundwork for enhanced communication, cooperation, and coordination.

Finding 3.h. Certain existing statutes, regulations, and sentencing guidelines do not provide sufficient sanctions to deter criminal or civil violations related to the import and export of goods and contraband, fraud, cargo theft, and other non-drug-related crimes.

Recommendation 3. Modify, to the extent feasible, the existing databases of federal agencies with significant regulatory and enforcement missions at seaports to ensure the collection and retrievability of data relating to crime with a nexus to seaports.

Recommendation 4. Evaluate the feasibility of capturing data on cargo theft offenses (including cargo theft taking place outside of seaports) through the National Incident-Based Reporting System. The Criminal Justice Information Services Advisory Policy Board should take the lead in the development, management, and continued evaluation of cargo theft to facilitate the data collection required to assess the nature and extent of cargo theft reporting and facilitate databasing. This will ensure that such information provides the maximum utility to its intended users.

Recommendation 5. Prepare, on an annual basis, comprehensive interagency crime threat assessments for seaports with international trade to support coordinated operational planning and enforcement activities as appropriate. All federal, state, and local law enforcement agencies with significant regulatory and enforcement missions at seaports with international trade, including Customs, Immigration, the Food and Drug Administration, the Environmental Protection Agency, the Bureau of Alcohol, Tobacco, and Firearms, the Drug Enforcement Administration, the FBI, the Coast Guard, and the Departments of Agriculture, Commerce, and Labor, should participate on a joint basis. The Intelligence Community should, to the extent allowed by law, support these threat assessments. Customs should coordinate this initiative, and should consider providing a sanitized version of the crime threat assessment to the private sector.

Recommendation 6. Promote enactment as soon as possible of the 21st Century Law Enforcement and Public Safety Act, which includes proposals for the creation of new criminal violations and enhanced penalties related to seaport crime. Additionally, federal agencies—including Customs, Commerce, Health and Human Services, Environmental Protection Agency, and others—should work with the Department of Justice to identify needs for new statutes and forfeiture provisions, including stiffer civil and criminal penalties for import- and export-related seaport crime. Justice should take the lead in this initiative.

Chapter 4: Threat Posed by Terrorism

There is no single, universally accepted definition of terrorism. The Code of Federal Regulations defines it as "...the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (28 CFR, Section 0.85).

Both within the United States and worldwide, the numbers of terrorist attacks are decreasing, but the numbers of casualties and the levels of property damage are on the rise. Within the United States, for example, the FBI recorded 5 terrorist incidents and 12 preventions of terrorist acts in 1998, down from 13 terrorist incidents or suspected incidents and 23 preventions in 1985. Worldwide, the State Department recorded a drop in the number of terrorist attacks from 302 in 1997 to 273 in 1998. But during both periods there was a dramatic rise in the numbers of casualties and the levels of destruction.

The most dramatic examples of these trends, and of the potential threats that international and domestic terrorists pose within the United States, are the bombings of the World Trade Center in New York City in February 1993 and of the Alfred P. Murrah Federal Building in Oklahoma City in April 1995. Prime examples outside U.S. borders are the August 1998 bombings of the U.S. embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, which involved highly destructive terrorist attacks that maximized property damage and casualties.

A more recent example of the potential threat in the United States was the arrest, in December 1999, of individuals attempting to enter the country from Canada. One subject, an Algerian-born man named Ahmed Ressam who was attempting to enter the country at Port Angeles, Washington, was stopped by U.S. Customs inspectors as he disembarked a commuter ferry from Vancouver, British Columbia. The inspectors found more than 100 pounds of urea sulfate in his rented vehicle, as well as approximately eight ounces of a highly volatile nitroglycerine mixture and fusing components. The FBI is currently investigating possible accomplices as well as possible links between these individuals and international groups.

The FBI divides the U.S. terrorism threat into two broad categories—domestic and international. Each of the five terrorist incidents recorded in the United States in 1998 was attributed to domestic terrorists. These incidents were bombings at a superaqueduct and two separate bank offices in Puerto Rico, a bombing at a women's health clinic in Birmingham, Alabama, and arson at a ski resort in Vail, Colorado, that resulted in $12 million in damages. There have been no successful incidents of international terrorism in the United States since the bombing of the World Trade Center in 1993.

The National Response to Terrorism

President Clinton has taken a strong leadership role in establishing a comprehensive and formal structure to deal with the terrorist threat. As a result of several important studies related to terrorism, strong direction has been provided to the Executive Branch through Presidential Decision Directives (PDDs).

Combating terrorism can be divided into three fundamental activities: crisis management, consequence management, and protective measures. National-level responsibilities for crisis and consequence management are clearly delineated in PDDs 39 and 62. PDD 63 addresses critical infrastructure protection to develop plans coordinated through the lead federal agencies for crisis and consequence management, eliminate vulnerabilities, prevent terrorist attacks, and, as necessary, respond to terrorist incidents. Specific security recommendations are addressed in Chapter 5.

PDD 39 designates the Department of Justice (acting through the FBI) as the lead agency in responding to terrorism in the United States. The Department of State is the lead agency in responding to acts of terrorism outside the United States involving American citizens or interests. The Federal Aviation Administration is the lead federal agency for coordinating the law enforcement response involving aircraft piracy (including terrorist hijackings) while an aircraft is in flight. PDD 39 divides the federal response to terrorism into two categories—crisis management and consequence management. Crisis management involves dealing with the causes of a terrorist attack; consequence management involves the aftermath of an attack. According to PDD 39, the FBI will lead the crisis management phase of a terrorist attack, and the Federal Emergency and Management Agency will lead the consequence management phase, utilizing the Federal Response Plan.

PPD 39 specifies that steps be taken to reduce U.S. vulnerabilities to terrorism. Major responsibilities among federal agencies for reducing vulnerabilities are delineated as follows:

- The Attorney General shall chair a Cabinet committee to review the vulnerability to terrorism of government facilities in the United States and critical national infrastructure.
- The FBI, as head of the investigative agency for terrorism, shall reduce vulnerabilities by an expanded program of counterterrorism.
- The Secretary of State shall reduce vulnerabilities affecting the security of all personnel and nonmilitary facilities abroad.
- The Secretary of Defense shall reduce vulnerabilities affecting the security of all U.S. military personnel.
- The Secretary of Transportation shall reduce the vulnerabilities affecting security of all airports in the United States and all aircraft and passengers and all maritime shipping under U.S. flag or registration or operating within U.S. territory and shall coordinate security measures for rail, highway, mass transit, and pipeline facilities.
- The Secretary of State and the Attorney General shall use all legal means available to exclude aliens who pose a terrorist threat.
- The Secretary of the Treasury shall reduce vulnerabilities by preventing unlawful traffic in firearms and explosives, by protecting the President and other officials against terrorist attack, and through the enforcement of laws controlling the movements of assets, and the export from or import into the United States of goods and services.
- The Director of the Central Intelligence Agency shall lead the intelligence community to reduce U.S. vulnerabilities to international terrorism through an aggressive program of foreign intelligence collection, analysis, counterintelligence, and covert action.

PDD 62 designates a National Coordinator for Counterterrorism and Infrastructure Protection in the National Security Council staff. The National Coordinator is tasked with coordinating the responsibilities of the federal agencies involved with

combating terrorism, estimated to be 47 in a recent General Accounting Office report.

PDD 63 outlines the federal government policy and responsibilities in Critical Infrastructure Protection. Based on the recommendations of the Presidential Commission on Critical Infrastructure Protection, PDD 63 divides the nation's infrastructure into 7 sectors, including transportation, and assigns lead agency responsibilities. While not specifically addressing the prevention of terrorism and focusing on cyber threats, PDD 63 includes protective measures as part of its menu of ways in which to protect the critical infrastructure.

While PDDs 39 and 62 clearly identify the FBI as the lead federal agency for responding to terrorism, they do not clearly designate a lead agency on developing security policy and procedures to protect seaports from acts of terrorism. In seaports, several federal agencies have existing authorities and responsibilities that lend themselves to filling that role: the Coast Guard, Customs, and Immigration. Of these agencies, the Coast Guard has, through its Captains of the Port, the broadest port security authority. Although Customs also has broad authority for security, its authority rests only in ports with international trade and/or passengers; the Coast Guard's authority also covers ports that handle only domestic vessels (see Chapter 2). Findings and recommendations regarding lead agency designations for port security are in Chapter 5.

The National Infrastructure Protection Center combines the involvement and expertise of numerous agencies in an effort to detect, assess, warn of, and respond to unlawful acts that threaten the nation's infrastructure. The Center was established in 1998 and is located at the headquarters building of the FBI. It employs representatives from the Department of Energy, the Department of State, the Secret Service, the Postal Service, and other federal and state law enforcement agencies. The National Infrastructure Protection Center monitors both cyber threats and, to a certain extent, physical threats. Physical threats are referred to the FBI's counterterrorism program, in view of the FBI's lead in countering terrorism in the United States. The National Infrastructure Protection Center is divided into three sections:

- The Computer Investigations and Operations Section performs three basic functions. It program-manages computer intrusion investigations conducted by FBI field offices; provides subject matter experts, equipment, and technical support to cyber investigators in federal, state, and local government agencies; and provides a cyber emergency response capability to help resolve cyber incidents.
- The Analysis and Warning Section provides analytical support during computer intrusion investigations and performs long-term analysis of threats and trends. This section provides warning of potential vulnerabilities and threats to government, state, local, and private sector entities.
- The Training, Outreach, and Strategy Section coordinates the training and education of cyber investigators within FBI field offices and other federal, state, and local agencies. It also coordinates outreach efforts to private sector companies, state and local governments, other government agencies, and FBI field offices, and it provides National Infrastructure Protection Center input into national planning processes.

Threat Assessment for U.S. Seaports

Although seaports represent an important component of the nation's transportation infrastructure, there is no indication that they are currently being targeted by terrorists. The FBI considers the present threat

of terrorism directed at any U.S. seaports to be low, even though their vulnerability to attack is high. The Commission believes that such an attack has the potential to cause significant damage.

Each year, thousands of ships, and millions of passengers, enter and leave the United States through seaports. It is estimated that 95 percent of the cargo that enters the country from noncontiguous countries does so through its seaports. In addition, many U.S. seaports are located adjacent to, or in, major metropolitan areas. A terrorist act involving chemical, biological, radiological, or nuclear weapons at one of these seaports could result in extensive loss of lives, property, and business, affect the operations of harbors and the transportation infrastructure (bridges, railroads, and highways) within the port limits, and cause extensive environmental damage.

In 1995 and 1996, Congress held hearings on the threat posed by the international proliferation of weapons of mass destruction (WMD). The findings of those hearings indicated that chemical, biological, radiological, or nuclear weapons, materials, and know-how are more widely available to terrorists now than at any other time in history. There are indications that some nations and rogue terrorist elements (of both domestic and international orientations) are actively pursuing the capability (or access to the capability) to use weapons of mass destruction in future attacks. These hearings also identified shortcomings in U.S. preparations for responding to weapons of mass destruction-related attacks on U.S. soil.

The FBI recognizes the risks and dangers posed by chemical, biological, radiological, or nuclear weapons and international organizations seeking to procure such weapons. However, it should be noted that the FBI and other federal, state, and local agencies have expended significant time and resources to obtain the equipment, training, and expertise needed for a response. This is a long-term process that continues to evolve under the direction of existing inter- and intra-agency programs. In addition, an overarching crisis management structure is in place to meet the unique demands of a chemical, biological, radiological, or nuclear event.

Today's terrorists have potential access to weapons and technologies that pose a serious threat to the U.S. population. The 1995 sarin gas attacks on the Tokyo subway system, which killed 12 people and forced more than 5,000 to seek medical treatment, marked the first large-scale use of a chemical agent by a terrorist organization. In 1985, an obscure religious cult in the American Pacific Northwest placed a biological agent in the salad bar of a local restaurant, causing dozens of people to become ill. The cult was attempting to influence a local election by affecting voter turnout. As these cases demonstrate, chemical and biological agents offer terrorists alternatives to conventional weapons such as bombs and firearms.

Another area of growing concern to the intelligence and law enforcement communities is the potential for widespread destruction and disruption resulting from attacks on vital infrastructure. A broad-based terrorist attack on targets such as power grids, water facilities, or transportation systems could temporarily paralyze a metropolitan area. In recent years, Algerian extremists have detonated bombs on the Paris subways, the Irish Republican Army has waged a campaign against Britain's passenger trains and subways, and Palestinian terrorists have carried out suicide bombings on Israel's buses. In the United States, unknown subjects derailed a passenger train in Arizona in 1995, and domestic extremist groups have attempted to attack military facilities and other critical infrastructures. In addition, as discussed previously, three of the five terrorist incidents recorded by the FBI in 1998 stemmed from terrorist attacks on critical

infrastructure targets (a superaqueduct project and two separate bank branch offices) in Puerto Rico.

While there is no evidence of an increased threat of terrorist attacks in America's seaports, the vulnerability of those ports is high. The influx of goods through U.S. ports provides a venue for the introduction of a host of transnational threats into the nation's infrastructure. Further, the nexus of transportation modes as well as the concentration of passengers, high-value cargoes, and hazardous materials make our ports potential targets for terrorist attacks. A chart reflecting a vulnerability analysis of the 12 seaports surveyed by the Commission appears at the end of this discussion in this chapter.

The current threat assessment of terrorism at U.S. seaports can be summarized as follows:

- The threat of terrorism on U.S. soil, including U.S. seaports, is low but should not be discounted. The United States has recorded several important successes against terrorism in recent years, but it remains a target of domestic and international terrorists. The August 7, 1998, bombings of the U.S. embassies in East Africa, and the subsequent August 20 U.S. missile attacks on suspected terrorist facilities in Afghanistan and Sudan, have heightened risks to U.S. interests worldwide. Generalized threats to U.S. interests have been issued by terrorist groups since the August 20 airstrikes. On June 7, 1999, international terrorist Usama Bin Laden, alleged mastermind of the U.S. embassy bombings, was placed on the FBI's Top Ten Most Wanted Fugitives list. Although there is no specific, corroborated threat information, the addition of Bin Laden to the "Top Ten" list heightens the potential for an act of terrorism.
- Threats of chemical or biological assault could represent an emerging issue for national infrastructure systems such as seaports, and would be consistent with a recent nationwide increase in the number of hoaxes involving threatened use of weapons of mass destruction. In 1997, the FBI investigated 74 cases involving use or threatened use of weapons of mass destruction. In 1998, it investigated 181 such cases. The vast majority (but not all) of these cases were found to be hoaxes. Hoax threats involving weapons of mass destruction continue to plague communities and to tax law enforcement resources.

Improved Response to Terrorism at the Seaport Level

Responding to terrorism is a multidisciplinary effort that involves prevention of potential acts, investigation of acts that do occur, and crisis and consequence management. Therefore, a comprehensive response to terrorism involves the efforts of law enforcement and intelligence agencies, emergency response agencies, and, when necessary, even the military. While Presidential Decision Directives 39, 62, and 63 provide overarching guidance to the federal government for crisis management, consequence management, and infrastructure protection, guidance for preventative measures is not so clearly laid out.

Further, the operational and jurisdictional challenges that are unique to the maritime and port environment add complexity to coordination and training efforts. These include the public/private interface; the intermodal nature of ports; the critical role of commercial ports in national security in terms of both military utility and economic vitality; foreign-flag shipping; multiple jurisdictions at all levels of government; and border control issues. Adding to the complexity of combating terrorism in U.S. ports is the variety of management arrangements at the ports—some have a robust port authority, some have strong local or

state oversight, and some are managed by private entities. Given these complexities and variations among ports, it is particularly challenging to identify issues and solutions that are applicable to all ports.

In some cases, U.S. seaports and their adjacent territorial waters are near the territorial waters of other countries. Operations in an interterritorial environment present additional challenges, such as coordinating enforcement activities and monitoring shipments through free-trade zones.

Many officials with whom Commission members spoke stated that law enforcement coordination and counterterrorism training at their seaports is satisfactory. Officials at other ports are not as confident in the level of coordination and training. Overall, there appears to be a need for an overall assessment of the training needs for seaport personnel to raise their awareness of terrorism issues.

Currently, 26 Joint Terrorism Task Forces are in place in communities around the country, including Philadelphia, New York City, Newark, Los Angeles, and South Florida. These Joint Terrorism Task Forces—headed by the FBI and made up of veteran investigators from federal, state, and local agencies—provide an integrated approach to counterterrorism efforts in their communities. In some locations that lack a Joint Terrorism Task Force, officials have established liaison efforts through which unclassified terrorist threat advisories and alerts are shared.

Joint Terrorism Task Forces contact port authorities, along with officials connected with other critical infrastructures, for the purpose, among other things, of conducting a terrorism threat assessment. An assessment is then made for the area covered by the Joint Terrorism Task Force, including seaports. This process, however, does not appear to take into consideration the unique environment of the seaport. Specific threat assessments for seaports are not conducted.

Cruise line security managers routinely receive threat warning information through the FBI's National Threat Warning System via the Coast Guard and directly through the Awareness of National Security Issues and Response system for commercial enterprises. In addition, state and local law enforcement agencies throughout the nation receive unclassified threat information from the FBI via the National Law Enforcement Telecommunications System.

Further, the maritime industry, including port authorities, routinely receives threat advisories issued by Coast Guard headquarters and disseminated by the local Coast Guard Captain of the Port. These advisories are based on information received from the Department of Transportation's Office of Intelligence and Security.

Communication of critical threat and intelligence information is largely a function of federal agencies (notably the FBI or the Coast Guard), which receive the information and then relay a sanitized version on a need-to-know basis. Communication is especially effective where Joint Terrorism Task Forces exist and state and local members hold security clearance.

In general, the threat warning systems (National Threat Warning System, Awareness of National Security Issues and Response System, and National Law Enforcement Telecommunications System) appear to be satisfactory and operating as intended. However, where these avenues of communication exist, much of the critical information is classified and therefore not readily releasable to civilian entities within the port. Some port organizations, from port authority law enforcement personnel to terminal operators, expressed frustration with not being aware of threat information on an ongoing basis.

Currently, Coast Guard Captains of the Port maintain Maritime Counterterrorism Plans that outline Coast Guard responsibilities and actions to be taken in the event of a terrorist incident or threat. These plans also

detail the roles and responsibilities of other key agencies, including the FBI, and summarize the existing memorandum of understanding between the Coast Guard and the FBI in matters concerning maritime terrorism as well as the interagency agreement between the Coast Guard and the FBI on maritime law enforcement. However, no requirement now exists for the Captains of the Port to coordinate or exercise the Maritime Counterterrorism Plans with other federal, state, or local agencies.

The proceeds from smuggling operations may be used to fund other terrorist activities. In South Florida, terrorist organizations have used seaports to smuggle narcotics and other contraband into the United States. The same organizations have exported stolen property, currency, and small arms. In the ports of Los Angeles and Long Beach, groups of Middle Eastern origin have exported weapons and high tech equipment to the Middle East. In Detroit, terrorist groups have used proceeds from stolen vehicles and from counterfeit videos as a source of funds. While the opportunity for smuggling by terrorist groups exists in Gulfport, New Orleans, and San Juan, no cases of such smuggling via those ports have been confirmed.

At present, there is minimal use of container screening technology (used primarily to detect cargo theft/smuggling) at U.S. seaports. In addition, the procedures/logistics employed to get the containers to the inspection sites do not provide adequate assurances that the cargo has not been tampered with, enabling potential smugglers to access contraband, weapons of mass destruction, and precursor material before it is inspected. In addition, federal inspectors inspect only a minimal amount of cargo.

The Coast Guard manages the National Security Council-directed Special Interest Vessel program, in which ships of countries known to sponsor terrorism are prohibited from entering U.S. waters. Ships of other selected countries are required to obtain prior permission (seven days in advance) to enter U.S. ports or are required to provide advance notices of arrival (up to three days) beyond the 24-hour standard requirement. The program also applies to citizens of targeted countries sailing on nontargeted ships.

While the potential was present at all ports surveyed, the probability that a terrorist subject would enter through a seaport varied among the ports. In South Florida, law enforcement officials speculated that as security tightens at U.S. airports, terrorists might use seaports as a point of entry. Seaports are particularly vulnerable to illegal entry because good screening processes are not in place. This issue is discussed in more detail in Chapter 5.

The smuggling of contraband and illegal aliens may be connected with terrorism issues. Many of the seaports the Commission surveyed did not employ any standardized background screening of seaport personnel. With the exception of the cruise ship industry, there are no attempts to screen personnel who have access to restricted areas of ship terminals. This situation could increase the risk that terrorists or other criminals are working in sensitive areas at the seaports. These and other security issues are discussed in more detail in Chapter 5.

The following chart reflects the findings of a vulnerability analysis of the 12 seaports surveyed by the Commission.

	Seaport											
Vulnerabilities	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
Port Facility Characteristics												
Current threat analysis availability	X	X	X	X				X		X		X
Port accessibility:												
Uncontrolled access									X			
Limited access	X	X			X	X	X	X		X		X
Controlled access			X	X							X	
Passenger terminal volume:												
High (over 100,000)	X	X	X					X			X	X
Medium (10,000-100,000)					X							
Low (10,000)				X		X	X			X		
DoD assets within port		X		X				X	X			X
Port Security Force Characteristics												
No security guard force												
Security manager, no guard force												
Security manager, security force with little/no training					X	X	X				X	
Security manager with trained security force, but not fully equipped				X								
Security manager with trained and fully equipped security personnel	X								X	X		
Security manager with trained, fully equipped security personnel and security exercises conducted on a regular basis		X	X					X				X
Physical Security Characteristics												
Landside												
No landside physical security measures												
Perimeter fencing, landside lighting only							X	X				
Fencing, lighting and live surveillance/patrol system	X	X			X	X			X		X	X

	Seaport											
Vulnerabilities (cont.)	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
Fencing, lighting and electronic surveillance system												
Fencing, lighting, electronic and live surveillance system			X	X						X		
Waterside												
No waterside security measures	X	X			X	X	X		X	X	X	X
Waterside lighting only								X				
Live surveillance only			X	X								
Single electronic surveillance system												
Multiple electronic surveillance systems												
Physical Characteristics of the Port												
Terrain												
Built-up, commercial	X	X	X	X	X	X	X	X	X	X	X	X
Mountainous, forested, undeveloped												
Open clear area/underdeveloped farm land												
Routes of access/egress												
Expressways		X	X	X	X			X				X
Major highways	X						X			X	X	
City streets						X			X			
Rail accessibility												
Rail gates open at all times								X	X			
Rail gates open only when in use	X	X	X	X	X	X	X			X		X
Unused rail access												
No rail access											X	
Water channels												
More than 3 choke points					X			X				X
1-3 choke points	X	X	X	X		X	X		X	X	X	
No choke points												

	Seaport											
Vulnerabilities (cont.)	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
Communications at Port Facility												
No communications readily available											X	
Communication interoperability between port & local law enforcement												
Non-secure					X	X	X	X		X		X
Secure									X			
Communication interoperability between port, federal, state & local law enforcement												
Non-secure	X	X	X	X	X	X						X
Secure												
Sustainability of Additional Port Resources												
High threat												
1 day		X	X	X					X			
3 days	X											
7 days					X	X		X		X		X
Indefinite							X				X	
Medium threat												
1 day		X		X								
3 days			X			X			X			
7 days	X				X			X		X		X
Indefinite							X				X	
Low threat												
1 day												
3 days												
7 days												
Indefinite	X	X	X	X	X	X	X	X	X	X	X	X

	Seaport											
Vulnerabilities (cont.)	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
Response Time for Specialized Security Personnel												
Police patrol												
30 minutes or less	X	X	X	X	X	X	X	X	X	X		X
30-60 minutes											X	
60 minutes or more												
Bomb squad												
30 minutes or less	X	X					X	X				X
30-60 minutes					X	X				X		
60 minutes or more			X	X					X		X	
SWAT												
30 minutes or less	X	X		X			X				X	X
30-60 minutes					X	X		X	X	X		
60 minutes or more			X									
Response Time for Specialized Emergency Personnel												
Fire department												
15 minutes or less	X	X	X	X	X	X	X	X	X	X	X	X
15-45 minutes												
45 minutes or more												
Pollution response team												
15 minutes or less		X		X			X	X			X	X
15-45 minutes	X		X		X					X		
45 minutes or more						X			X			
Proximity to Urban Areas												
Population over 100,000	X	X	X	X	X	X		X	X	X	X	X
50,000-100,000							X					

	Seaport											
Vulnerabilities (cont.)	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
Geographical Location												
OCONUS											X	
East/west coast	X	X	X	X	X					X		
Gulf coast							X	X				
Alaska, Hawaii, Northwest, Central or New England						X			X			
Proximity to International Borders												
High threat												
Medium threat												
0-100 miles												
101-500 miles												
+500 miles					X							
Islands											X	
Low threat												
0-100 miles	X	X	X	X		X						
101-500 miles									X			
+500 miles							X	X		X		
Islands												

Note: “X” indicates “yes.”

Findings and Recommendation

Finding 4.a. There is a formal structure at the national level to deal with the terrorist threat that clearly delineates responsibilities among federal agencies.

Finding 4.b. Coordination among law enforcement agencies at all levels of government is generally good where FBI Joint Terrorism Task Forces are located to coordinate the exchange of information and joint investigations. However, the Joint Terrorism Task Forces do not typically focus on activity in seaports. The extent of coordination (among non-law enforcement agencies and key private sector entities) related to counterterrorism security measures is inconsistent at the 12 seaports surveyed.

Finding 4.c. Federal officials do not conduct annual, seaport-specific terrorism vulnerability and threat assessments that might assist seaports in preparing for terrorist threats.

Finding 4.d. Risk management for individual seaports can be effectively carried out only by federal agencies in conjunction with local officials.

Finding 4.e. Many Coast Guard Captains of the Port have existing Maritime Counterterrorism Plans. But these plans are developed with insufficient coordination and input from other agencies, and there is no requirement that they be exercised.

Finding 4.f. In general, most seaport personnel are not aware of, or sensitized to, terrorism issues. Most have not received training and therefore are not aware of the appropriate initial response to terrorism.

Finding 4.g. Improved security and cargo detection technology could assist in identifying high risk shipments.

Finding 4.h. The threat of terrorism on U.S. soil, including U.S. seaports, is low but should not be discounted.

Finding 4.i. U.S. seaports are vulnerable to terrorist attacks, and such attacks have the potential to create substantial damage to seaport infrastructure, with significant national security consequences.

Finding 4.j. Threats of chemical or biological assault could represent an emerging issue for national infrastructure systems such as seaports.

Recommendation 7. Intensify the federal government efforts to assist seaports in preparing for the possibility of terrorist acts directed at critical infrastructure. Specifically, the Department of Transportation, as Lead Sector Agency for Transportation in accordance with Presidential Decision Directive 63, should be responsible for coordinating implementation of the following recommendations:

- On an expedited basis, the Coast Guard and the FBI (including the National Infrastructure Protection Center), in coordination with other relevant agencies and the private sector, should develop a system for categorizing seaport physical and information infrastructure based on both vulnerability and threat (e.g., low, medium, and high risk).
- The federal government should establish baseline vulnerability and threat assessments for terrorism at U.S. seaports as soon as possible. Priority should be given to the Strategic Seaports, Presidential Decision Directive 40's "Controlled Ports," and economically strategic seaports, the criteria for which should be developed by the Interagency Committee on the Marine Transportation System/Marine Transportation System National Advisory Council. Thereafter, threat and vulnerability assessments should be conducted every three years. The FBI should ensure that seaports are included within its field offices' domestic terrorism surveys to

assess the potential threat. The Coast Guard should conduct port vulnerability assessments. Both the FBI and the Coast Guard should coordinate their efforts with other agencies, particularly the Department of Defense, for the Strategic Seaports for large-scale military mobilization, and for those designated as Controlled Ports under PDD 40. Results should be made available, as appropriate, to all relevant agencies and local port security committees.

- Coast Guard Captains of the Port and the FBI should ensure that their respective Maritime Counterterrorism Plans and Incident Contingency Plans are updated and coordinated annually, and exercised regularly with other concerned federal, state, local, and private entities.

Chapter 5: Security Practices in U.S. Seaports

A primary objective of the Commission was to assess the overall state of security in U.S. seaports. Chapter 2 discussed the nature of seaports and the interactions of federal, state, and local government officials and private sector entities. Chapter 3 covered the nature and extent of crime at seaports and Chapter 4 addressed the specific crime of terrorism. Crime is a serious threat at the seaports. The threat of terrorism is low, but the vulnerability of seaports to terrorism is high. Security is a key to providing some level of deterrence. Chapters 3 and 4 examined the relationship between lack of seaport security and exploitation of the seaport by the criminal element.

This chapter focuses on the current state of security in our seaports and the associated issues of custodial and informational control over the cargo, passengers, and vessel crew members that enter and leave through the nation's ocean gateways. This focus is based on observations made by the Commission during its on-site assessments at the 12 seaports surveyed. It also includes information gathered through a series of focus group meetings with federal agency representatives, port authorities, law enforcement and private security personnel, and representatives of key sectors of the maritime industry. This chapter analyzes port security by looking at physical security and access control; security of cargo, passengers, and crew; and security for military mobilization operations in commercial seaports. It begins with a discussion of threat and vulnerability as the primary components for assessing the degree of the security risk present at U.S. seaports.

Management of Risk

Before assessing security at the 12 seaports surveyed in this report, a review of the nature of risk, threat and vulnerability may be helpful. Although the model below was developed primarily to address the threat of terrorism, it is applicable to all threats to seaport security. According to the Coast Guard, risk management should take into account the vulnerability of a facility, the level of threat against it, and the impact if an attack were successful. A simple formula is:

Risk = Vulnerability x Threat x Consequence

Threat is the intent to inflict injury or damage. It is an important concept because whether one is dealing with a wartime scenario, a civil disturbance, terrorism, or other intentional acts, threat assessments can indicate how likely it is that an act will be carried out against a vessel or a port facility. Security planning and resource management must consider potential threats to ports and assess how a port's destruction or damage might have military, economic, political, or publicity value to an attacker. While the numbers of domestic maritime terrorist or subversive acts have been few, the vulnerability of many U.S. seaports is quite high.

Vulnerability is defined as the susceptibility of an asset or group of assets to an adverse action or potential action through which the effectiveness of the asset is

reduced or eliminated. While no measure exists that can determine absolute vulnerability, tools and methods are available for determining relative vulnerability of various port facilities, and these can aid in setting priorities for employment of limited security resources. Factors to be considered in determining vulnerability include, but are not limited to, the following:

- Geographical location and avenues of ingress and egress.
- Accessibility of the vessel or facility to disruptive, criminal, subversive, or terrorist elements.
- Adequacy of storage facilities and ease of access to valuable or sensitive items such as hazardous materials, arms, ammunition, and explosives.
- Availability and adequacy of security forces and adequacy of physical security measures.
- Adequacy of coordinated planning and operations among responsible agencies and private port entities.

Consequence is the adverse effect from the loss of an asset, and assessing its important in security planning. An asset with low threat and vulnerability but whose loss would result in extremely serious consequences may deserve more attention than another where the threat and vulnerability may be high but the negative impact of its loss or damage would be low. In evaluating the risk to an asset, consideration must be given to its mission sensitivity, its importance to the continuity of essential port operations, and the military or economic impact of its loss or damage. While no attempt has been made to develop a relative scale of consequence, high-value assets may include:

- Production, supply, and repair facilities such as power generating stations, oil and chemical storage facilities, and shipyards.
- Transfer, loading, or storage facilities such as rail and truck terminals, cargo container yards, airports, vessel docking facilities, and loading facilities.
- Transportation modes, such as trains, trucks, aircraft, vessels, conveyors, and pipelines and their consolidation (choke) points.
- Transportation support systems such as bridges, tunnels, runways, roads, locks, piers, channels, anchorages, and aids to navigation.

Much of what the President's Commission on Critical Infrastructure Protection considered was the relationship between vulnerability and consequences and conceptual ways to approach risk management using the formula above.

Presidential Decision Directive 63 notes the findings of the President's Commission on Critical Infrastructure Protection, including the vulnerability of the nation's infrastructure, of which maritime ports are a part. The President's Commission on Critical Infrastructure Protection specifically notes:

> We know our infrastructures have substantial vulnerabilities to domestic and international threats....Although we know these new vulnerabilities place our infrastructures at risk, we also recognize that this is a new kind of risk that requires new thinking to develop effective countermeasures....The Commission has not discovered an immediate threat sufficient to warrant a fear of imminent national crisis. However, we are convinced that our vulnerabilities are increasing steadily, that the means to exploit those weaknesses are readily available, and that the costs associated with an effective attack continue to drop.

The National Security Strategy echoes the findings of the President's Commission on Critical Infrastructure Protection by stating that "...advances in information technology and competitive pressure to improve efficiency and productivity have

created new vulnerabilities to both physical and information attacks as these infrastructures have become increasingly automated and interlinked." It further "makes it U.S. policy to take all necessary measures to swiftly eliminate any significant vulnerability to physical or information attacks on our critical infrastructures...."

The National Security Strategy and the President's Commission on Critical Infrastructure Protection clearly recognize the vulnerability-based risk management required in preventing asymmetric or terrorist attacks on our infrastructure. Contributing to this finding is the difficulty in assessing threats from unconventional, ad hoc terrorist groups with no state sponsor and the associated threat-warning problem inherent in addressing those threats.

Threat-driven risk management is inherently dependent on indicators that are part of a robust warning system. The challenge of combating terrorism, particularly with the rise of non-state-sponsored groups and ad hoc groups, is complicated by the difficulty of establishing indicators and warning thresholds for such nebulous groups

Terrorist *threats* to U.S. interests are traditionally evaluated using several broad criteria regarding terrorist *groups*—their existence, history, intent, targeting, and security environment. In other words, groups that may conduct attacks are analyzed to gauge the threat of terrorism. For existing, state-sponsored groups, these criteria are valid and have proven successful. But the indications and warning process using existing indicators and evaluation tools collapses in the face of less-organized, ad hoc terrorist groups with shadowy connections and a loose or nonexistent base of support, such as the group of terrorists that bombed the World Trade Center. Therefore, threat-based risk management alone is not fully adequate.

In Chapter 4, the Commission concluded that the threat of terrorism on U.S. soil, including seaports, is low but should not be discounted. It also concluded that the vulnerability of seaports is high for the reasons stated above. Finally, it concluded that threats of chemical or biological assault could represent an emerging issue for national infrastructure systems such as seaports.

Security is measures taken to prevent terrorism and other criminal activity. Threats—particularly terrorist threats—are often unpredictable; security should be considered from a vulnerability-driven perspective rather than a threat-driven perspective. Recommendations that minimum port security guidelines should be developed are in line with this position. Guidelines, however, should be developed for varying threat levels, because threat warnings are applicable in some, but not all, situations.

Considering infrastructure protection from a vulnerability-driven perspective is appropriate and is in keeping with national guidance. This creates a powerful argument for minimum-security guidelines and lays the foundation for guidelines to be developed for varying degrees of threat.

Maritime Vulnerabilities

In 1998, the Department of Transportation initiated a Surface Transportation Vulnerability Assessment. The assessment found that the United States possesses an effective and efficient surface transportation infrastructure that promotes the well-being of its citizens as well as important economic and national security goals. The level of security afforded this infrastructure is relatively low compared with the security enhancements recently implemented in the commercial aviation sector. However, there is sufficient reason to believe that the security levels of the surface transportation modes need to be raised as the vulnerabilities of the current infrastructure become apparent.

The maritime mode does not exhibit a substantial security or anti-terrorism profile, particularly when compared with the emphasis commercial aviation places on these activities. The primary reason for this situation is historical. In the U.S. experience, aviation, particularly in an overseas environment, has been by far the most visible and dramatic transportation target for terrorism and violent criminal incidents. Few similar actual incidents involving domestic surface transportation assets have occurred. Thus, each mode has responded to its own specific security and terrorist history, and has developed and implemented security practices that are consistent with its actual and assessed vulnerabilities. Additionally, the open nature of the maritime environment makes it difficult, if not impractical, to apply security measures that would hinder the movements of individuals. However, the increase in the potential threat to these facilities in recent years is reason to review this situation.

An efficient and secure maritime transportation network is an integral part of U.S. national security. Both the military and the civilian economies depend on effective and secure marine transportation networks. Today's marine transportation system has adapted to a global-based economy and the demands of "just-in-time" delivery of cargo (scheduled arrival of spare parts timed to assembly line requirements), and in doing so is predominantly reliant on electronic data exchange for documentation of the many transactions associated with interstate and international transportation. As the pace and volume of global transportation changes, new opportunities are introduced that can be exploited by a broad scope of antagonists from pilferers to terrorists.

The operation of the U.S. economy depends on the effective movement of freight, the stability of intermodal connections, and the reliability of the transportation network. Any long-term disruption to the maritime transportation infrastructure could result in serious economic and strategic consequences regionally, nationally, and internationally. The criticality of shipping to support our armed forces abroad has become more apparent. As commercial users continually require faster and more extensive service, the maritime transportation network's efficiency, complexity, and inter-connectivity have grown. Maritime transportation providers, along with port and waterway facility operators, are implementing new information technologies and logistics practices responsive to changing business environments in which timely parts delivery plays an integral role. Greater nationwide sensitivity to on-time performance heightens the consequences of both delays and major disruptions.

Setting Standards of 'Adequate Security' for Seaports

The Commission found many publications that promoted security and provided guidelines. Some were published by the federal government, some by private sector firms, and some by trade associations. However, there were no generally accepted standards or guidelines to assist seaports in improving security. Without standards or guidelines, seaports have no benchmark to use if they choose to make a concerted effort to improve security. They also have no basis to measure the effectiveness of existing security measures. The absence of standards and guidelines also provided a dilemma for the Commission in carrying out its mission to assess security in seaports.

Before the Commission could assess seaport security, an "adequate security" baseline had to be established to compare against existing seaport security measures. Researching existing publications turned up four basic categories of measures: physical security and access control; passenger

and crew security; cargo security; and military mobilization security. In the Commission's efforts to develop its framework, it recognized one set of guidelines for seaport security that could be deemed "minimum guidelines" and a more complete set that could be described as "enhanced guidelines." Then the Commission developed criteria for each category. The two categories were developed in recognition of the fact that not all seaports require the same level of security. Seaports with a higher risk may need to consider additional security measures. Appendix B (Methodology) contains the criteria used in each of the categories.

Additionally, Appendix F is a conceptual framework for developing a "model port." It contains suggested attributes and potential best practices of a model port in the areas of physical security and access control, passenger and crew security, cargo security, and military mobilization security.

Assessment of Security at 12 Seaports

Assessing the state of seaport security is difficult. Unlike airports, seaports cannot be easily categorized. No two of the 361 public seaports in the United States are exactly alike. They have a broad range of characteristics. Many seaports are small and have limited commerce; only 144 process more than a million tons of cargo per year. In the larger seaports, the activities can stretch along a coast for many miles, including public roads within their geographic boundaries. The facilities used to support arriving and departing cargo are sometimes miles from the coast. The inland ports accept mostly bulk products such as grain, petroleum, coal, or steel. The seaports that accept international cargo have a higher risk of international crimes such as drug and alien smuggling. The top 50 ports in the United States account for about 90 percent of all the maritime cargo tonnage. In terms of container shipments, 25 U.S. seaports account for 98 percent of the cargo. Cruise ships visiting foreign destinations embark from 16 U.S. ports.

Given these difficulties, and taking into account the criteria discussed above, the Commission's assessment is that the state of security in U.S. seaports is generally poor to fair. This assessment of all U.S. seaports is an extrapolation of the state of security observed during our summer 1999 on-site surveys of the 12 domestic seaports, which constitute a representative cross-section of U.S. seaports. This assessment of U.S. seaport security is a result of comparing the Commission's on-site observations with the criteria for good and enhanced security discussed in Appendix B. Summary data supporting this assessment of seaport security are found in the table below.

The following table demonstrates that the level of security does not even meet the Commission's definition of minimum standards or guidelines. Some ports have been working diligently to improve security, but most have not. Several key issues are discussed below.

Minimum Security Standards

Although the Commission found during its port visits that there were no uniform minimum security standards (physical, procedural, and personnel) for seaports, some ports are making outstanding efforts to improve security. In Port Everglades, for example, the port authority, federal and local law enforcement agencies, and carriers are adopting standards (for fences, lighting, gates, etc.) in an effort to restrict access to the port and its operations.

By contrast, some ports do not even have fences around areas where cargo was loaded and unloaded. Other ports have put in security on a piecemeal basis as problems arose. The port officials we talked to from seaports that import automobiles have all put up sturdy fences with

Port Security Assessments	% of Ports in Affirmative
Overall Assessment of Current Security Measures	
Do security measures within the port meet the minimum port security criteria?	0
Do security measures within the port meet the enhanced port security criteria?	0
Vulnerability and Threat Assessments	
Has a vulnerability assessment been performed for the port?	17
Has a threat assessment been performed for the port?	0
Physical Security and Access Control	
Is adequate perimeter fencing (chain-link with barbed-wire top-guards) in place?	50
Is perimeter fencing surrounding vehicle storage areas reinforced with guard rails, concrete barriers, earth berms, or other means to prevent vehicles from being driven through the fence?	33
Are access points to marine terminals gated?	92
Are gates either locked or monitored by security personnel?	83
Are marine terminal security personnel uniformed for easy identification?	75
Do security personnel conduct patrols of the port or marine terminals?	67
Do security personnel receive specialized security training?	67
Is lighting for the port/terminal sufficient?	83
Is the carrying of firearms restricted within the port?	0
Is the access of personal vehicles to piers, terminals, etc., restricted/controlled?	50
Are employee parking lots separated from vessel loading or cargo storage yards?	42
Enhanced Measures	
Is a port-wide identification card system in place to control or restrict access?	8
Are criminal records checks performed on employees and dockworkers who have access to the port?	17
Are closed-circuit television cameras or other intrusion detection systems widely in use within the port?	0
Cargo Security	
Are cargo control and reconciliation procedures in place?	92
Are sound sealing practices followed?	75

Port Security Assessments (cont.)	% of Ports in Affirmative
Is access to equipment controlled?	42
Are sound cargo receipt/delivery/transfer procedures in place?	92
Is "loose" cargo properly stored?	83
Are shipping documents reviewed for accuracy?	92
Are measures taken to secure high-value merchandise?	83
Are sound personnel security practices followed?	67
Are procedures in place to audit irregularities and correct vulnerabilities?	33
Enhanced Measures	
Separate Federal Inspection Station for foreign cargo?	0
CCTV to record lading/unlading procedures?	0
Have installed automated access control systems to monitor access to restricted areas?	0
Employ non-intrusive technology to identify contraband and/or verify cargo shipments?	25
Trucking companies use automated system such as GPS to track trucks and shipments?	42
Firms implemented "Integrated Security Concepts" to deter internal conspiracies?	8
Passenger and Crew Security (7 Cruise Ship Ports Only)	
Are passenger and cargo operations segregated within the port?	100
Is there a dedicated passenger terminal for cruise ship operations?	100
Is the terminal operating company employed directly by the cruise lines?	43
Is passenger terminal security provided by a uniformed, private security force?	100
Is additional security available from port authority police?	71
Are embarking and disembarking passengers separated within the terminal?	86
Is appropriate passenger and baggage screening technology (x-ray and metal detector) employed at the passenger terminal?	100
Are gangways properly secured to prevent unauthorized access to vessels?	86
Do crew have up-to-date knowledge of passenger documentary requirements and check documents as passengers enter the terminal area?	86
Do terminal security personnel receive training in the performance of their duties?	71
Does the terminal security force receive terrorist threat information from federal, state, or local law enforcement agencies, or from the port authority?	43
Are security procedures coordinated between terminal and vessel personnel?	86

Port Security Assessments (cont.)	% of Ports in Affirmative
Enhanced Measures	
Is there a separate Federal Inspection Station where international passengers arrive?	0
Are automated access control cards used instead of keys to enter terminal facilities?	0
Are carriers using the Advance Passenger Information System and submitting information in timely fashion to Customs and INS so law enforcement checks can be done prior to vessel's arrival?	0
Military Mobilization (Applies to Only 4 of the 12 Seaports Surveyed)	
Is the port readiness committee active?	100
Are all applicable federal, state, local, and private sector entities included in the port readiness committee's membership?	75
Is there a written local memorandum of understanding on the port readiness committee?	50
Has a port readiness exercise been held in the past two years?	100
Enhanced Measures	
Have the "lessons learned"/problems from the last port readiness exercise been resolved?	50
Has a Defense Department vulnerability assessment been done?	25
Are there enough resources to coordinate the local port readiness committee process adequately?	50
Coordination and Cooperation	
Is there coordination between the port, law enforcement agencies, and the private sector or trade community regarding security issues?	17
Does labor cooperate with the port, the trade community, and law enforcement agencies regarding security issues within the port?	42
Is there cooperation between the federal agencies regarding security issues within the port or terminal?	42
Is intelligence being shared between law enforcement agencies within the port?	25
Technology	
Is any technology (e.g., X-rays, closed circuit TV) available in the port for the use of law enforcement agencies?	42
Is the port installing or implementing any special equipment (e.g., automated access systems, closed circuit TV) within the port?	8

guardrails and lighting because in their assessment auto theft was a serious problem and if the fences did not have guardrails, thieves would simply drive the cars right through the fences.

Some ports believe they do not have a theft problem and thus they do not need security. One port official repeatedly stated that there must be an economic justification for every cent he spends and because he did not perceive crime as a high threat, there was no justification for enhancing security. Another port official repeatedly said that federal crimes are the federal government's responsibility and if security is needed, then the federal government should provide it.

Some ports that have made major expenditures for security to support federal crime efforts, such as drug smuggling, believe they have been put at an economic disadvantage. They are of the opinion that spending millions on security to support federal crime issues increases their cost of doing business, which could have a long-term negative impact on business if other ports chose to ignore these issues.

Many officials we talked to recommended minimum security standards for seaports. Base-level uniform guidelines could include physical security (e.g., fences, lighting, gates), procedural security practices (for controlling the delivery, receipt, and movement of cargo), and personnel security standards (for identifying high-risk individuals who want access to sensitive areas within the seaport).

The absence of uniform minimum physical, procedural, and personnel security standards for seaports can result in security deficiencies or gaps, within and between seaports, that the criminal element can easily exploit. Where different standards are implemented at different seaports that share the same risk assessment or are in geographic proximity to each other, the results can invite "port shopping" by criminals.

Access Control to Seaports and Terminals

The Coast Guard has legislative authority for regulating waterway security and security for waterfront facilities, but may not have authority for other areas not located on the water. Customs can regulate any area where international cargo, passengers, or vessels arrive or are processed. It is not clear whether a federal agency has authority for regulating overall access to a seaport if the port handles only domestic cargo. Either agency could probably make a case for being able to regulate access control, however.

Common sense and generally accepted industry security standards dictate that personnel access to vessels, cargo receipt and delivery operations, and passenger processing operations be restricted or tightly controlled to reduce unauthorized access to sensitive areas and operations. Firms usually control or regulate employee and visitor access to operational areas through the use of identification cards. The absence of port-issued identification cards can permit unauthorized personnel to access vessels, cargo receipt and delivery operations, and passenger processing operations and facilities within seaports. The result can be an increase in crimes, such as drug smuggling and pilferage, in the port. The lack of identification cards can also affect the ability of businesses and law enforcement personnel to identify, and restrict the access of, employees with criminal records to sensitive areas in the port.

There are currently no established standards or regulations that require ports to issue identification cards to personnel as there are at other facilities such as airports. Also, there are no requirements that background checks be performed on personnel applying for access to sensitive areas.

Union officials have vigorously opposed any effort to require that criminal record checks be conducted on their members. Particularly on the West Coast, they state that no union member has been convicted

of drug trafficking or other felony offense. They believe these checks would violate their members' privacy.

These union officials are also against wearing identification badges. The union says that this issue has been under negotiation with management and the union officials do not want the federal government to interfere with the bargaining process.

During visits to the Port of Miami and Port Everglades, the Commission found that access to the seaport and its facilities (piers, terminals, warehouses, etc.) was controlled or restricted by the issuance of port-issued identification cards. These cards were issued to all regular workers (dockworkers, truck drivers, warehouse personnel, etc.). At these two ports, the company employing the workers submitted a letter advising the port that its employees regularly require access to the port or its operations. Upon receipt of the letter and payment of a processing fee (and contingent upon the completion of a successful criminal history check on the employee), the employee is issued a port-specific identification card. None of the other ports visited had identification card schemes in place, although the New York Waterfront Commission does perform criminal background checks on all waterfront workers.

During its visits the Commission also found that at many seaports (e.g., New Orleans, Gulfport, and Miami), the access of privately owned vehicles and commercial vehicles to vessels, cargo receipt and delivery operations, and passenger processing operations was not controlled. The lack of control permits individuals to park vehicles adjacent to vessel lading and unlading operations, cargo operations, and passenger arrival and departure areas.

The absence or lack of enforcement of security standards to restrict or control vehicle access increases the risk that criminals can easily gain access to sensitive areas. The proximity of uncontrolled vehicles to vessel, cargo, and passenger operations also increases the risk that violators could quickly remove large amounts of pilfered cargo or contraband. This has been a serious problem for some local authorities.

Although a number of ports have the appearance of physical access control, in many cases, access is freely granted to anyone seeking entry into the port. At a number of ports we were told that anyone arriving at a port entrance with a tractor was automatically waved through without being questioned. At other ports a simple statement of intent to go to a particular location was sufficient to gain access. In another port pedestrians could freely walk through access control points without being questioned.

The same *appearance* of control exists at terminal and container yards. Some are relatively secure. Others have controls in place that are easily overcome. For example, some container yards in San Juan have a "sticker system" which requires that a tractor have a designated letter sticker (A, B, etc.) to enter a particular yard. However, a driver without the appropriate sticker can have a confederate with the correct sticker enter the yard and haul the chassis outside the fence for later pickup.

A serious issue the Commission identified during its field visits related to firearms. At some seaports, such as New Orleans, local policy and/or agreements with the local labor force restricted the presence of firearms. At other ports, such as Miami, the carrying of firearms was not restricted or controlled. In airports, the presence of firearms is prohibited by federal regulations and local laws, which are enforced by federal, state, and local government agencies. In addition, the private sector, usually the airlines or airport authorities, hire contract security personnel to screen baggage, passengers, employees, and the public who require access to the "secure" side of the airport for weapons. The lack of laws restricting the carrying of firearms on seaports means that criminals,

including terrorists, can freely transport firearms onto seaports and can access cargo vessel and cruise line operations armed. The potential presence of armed criminals poses a serious threat to law enforcement personnel, workers, crewmembers, and passengers.

Cruise Ship Security

The vulnerability of passenger vessels and associated passenger terminals to terrorist attack has been a major national and international concern since the death of a U.S. citizen during the hijacking of the Italian cruise ship *Achille Lauro* in October 1985. To address this threat, the President signed into law the Omnibus Diplomatic Security and Antiterrorism Act of 1986, Title IX of which constitutes the Maritime and Port Security Act. That act amended the Ports and Waterways Safety Act (33 USC 1221) and authorized the Coast Guard to "carry out or require measures, including inspections, port and harbor patrols, the establishment of security and safety zones, and the development of contingency plans and procedures, to prevent or respond to acts of terrorism."

Also in 1986, the International Maritime Organization adopted and published its *Measures to Prevent Unlawful Acts against Passengers and Crews on Board Ships,* guidelines that apply to passenger ships engaged on international voyages of 24 hours or more and to the port facilities that serve them. Initially, the Coast Guard relied on voluntary compliance with these guidelines to ensure that passenger vessels and terminals were prepared to prevent and respond to acts of terrorism. However, voluntary compliance did not produce the industrywide level of security necessary to protect passengers and crews. Witnessing an increase in domestic terrorism, and in the threat of international terrorism, the Coast Guard in July 1996 published an interim rule requiring the development of security plans by passenger vessels and terminals.

The Coast Guard, after much consultation with the private sector, aligned its new regulations as closely as possible with the International Maritime Organization measures. These measure contain the basic elements needed to develop a sound security program while giving industry the flexibility to adapt security measures to different ports, passenger terminals, and vessels. These regulations, which were finalized in October 1998, required the development of security procedures ranging from hand searches to screening with X-ray equipment and metal detectors. The measures were designed to prevent the introduction of weapons, incendiaries, or explosives on board passenger vessels by persons, within personal articles or baggage, in stowed baggage, or among ships' stores. The regulations were made applicable to all passenger vessels over 100 gross tons, carrying more than 12 passengers for hire, and making voyages lasting more than 24 hours, any part of which is on the high seas (international waters). They apply to vessels for which passengers are embarked or disembarked in the United States or its territories, and to the passenger terminals that receive them.

The regulations, however, do not apply to ferries that operate on lakes, bays, and sounds, and that transit international waters for only short periods of time, on frequent schedules. Thus, many ferries or gambling ships that carry hundreds of passengers are not subject to these security regulations, but may be an attractive target to terrorists.

In its port visits and meetings with industry groups, the Commission found that security in place for passenger vessels and terminals is generally in compliance with the regulations. Today, passenger vessels and terminals are subject to the highest security requirements of all maritime transportation facilities. Passenger security plans prepared by private sector owners and operators are submitted to and examined by the Coast Guard, which routinely verifies that vessels and terminals are

operating in accordance with their specified security procedures and with applicable federal security regulations.

The cruise industry, whether operating overseas or from U.S. ports, is almost entirely foreign owned and operated, with ships registered in countries other than the United States. The International Maritime Organization's security measures for passengers and crews, strongly supported by the U.S. government, were a highly successful formulation of internationally agreed-upon technical measures to improve security and reduce the risk to passengers and crews. It was to maintain consistency with these international standards that the Coast Guard limited the scope of its security regulations to larger passenger vessels engaged in international voyages.

In this case, the use of regulated minimum standards was found to be necessary to protect cruise ship passengers. It should be noted that the regulations apply only to certain passenger vessels. There are a host of passenger vessels and ferries that are not subject to these rules and have not chosen to comply voluntarily.

Cargo Security

The private sector, including vessel carriers, terminal operators, trucking companies, warehouses, railroads, and importers and exporters, has a strong interest in maintaining security for cargo. However, the responsibility for the security of cargo changes as cargo moves through most seaports. Typically, vessel operators, or carriers, are responsible for the security of cargo as it is transported via the water from port to port. Once the vessel docks and unloads its cargo, though, the security of the cargo becomes the responsibility of the port authority or a terminal operator, which oversees the unlading of the cargo from the vessel and the movement of the cargo to a secure area under its control.

The port authority or terminal operator then oversees the delivery of the cargo to facilities such as warehouses, container freight stations, freight forwarders, importers, and railroads within the immediate area. Trucking companies usually move the cargo from the port authority or terminal operator's facility to warehouses or importers.

While the cargo is being transported from the port authority or terminal operator's facility to the other facilities, the trucking company is responsible for its security. Once the cargo is transported to a warehouse or a container freight station, the facility operator is responsible for its security.

While under the custody of the facility operator, the cargo may be subject to a variety of operations such as devanning, manipulation, storage, and repackaging. The cargo is then normally moved from the facility to the owner or importer by a transportation company (such as the facility operator, an independent trucking company, or the cargo owner). The transportation company is responsible for the security of the cargo until the owner or importer takes final delivery.

If security practices are lax at any of the cargo-handling facilities described above, or when cargo is being transported between facilities within a seaport, the cargo is vulnerable to theft, pilferage, and unauthorized access.

The Commission found that the several trade entities that operate in seaports (such as terminal operators, carriers, trucking companies, warehouses, and importers) were doing an excellent job at controlling cargo, while others were not. The members of the working group also found that few of the seaports or facilities employed measures or technology that enhanced cargo security.

During our reviews, the Commission working group found that seaports did not have separate and restricted areas where vessels, cargo, and passengers arriving

from foreign locations were processed. Frequently, cargo, vessels, and passengers arriving from outside the United States were processed adjacent to, or in the same areas as, those arriving domestically.

In contrast, airports are required to provide sterile, restricted areas for performing federal inspection activities (of aircraft, cargo, and passengers arriving from foreign countries) that are separate and distinct from domestic activities, and that comply with nationally accepted standards.

The lack of separate and distinct foreign and domestic operations processes within seaports can permit dock workers and other individuals with access to ports, such as truck drivers and vendors, to mix freely with operations involving foreign vessels, cargo, or passengers which they are not officially authorized to participate in. This unapproved access can increase the risk of illegal activities such as drug smuggling, cargo theft, pilferage, and alien smuggling. During the port surveys, federal officials also expressed concern about the lack of security for international cargo at the seaports and said that international cargo should not be mingled with domestic cargo, or tampered with, before federal inspection and release procedures. Areas where international cargo arrives and departs need to be controlled to prevent unauthorized access to the cargo.

Cargo control is an area that has been consistently emphasized by the Customs Service over the last decade. Because of the increased threat of drug smuggling in the 1980s, Customs developed several cooperative programs with the private sector. The first was the Carrier Initiative. In this program, Customs developed detailed cargo security standards for vessels and signed agreements with more than 1,000 carriers who agreed to abide by the rules in exchange for favorable consideration in the event that penalties were assessed against them. Customs later expanded the program for freight forwarders, brokers, importers, exporters and others involved in international trade. Under the name of America's Anti-Smuggling Coalition Initiative, Customs also included businesses from Latin American countries that were considered high risk for drug smuggling. This voluntary program has served to improve the practices of those businesses that chose to participate.

Import Cargo Control

As clearly stated in the previous section, good cargo security guidelines and vigorous terminal security and inventory control procedures at access points to a port facility (driver documentation check, pick-up and delivery order validation, shipment discrepancy recordation, closed circuit television, scales. etc.), in conjunction with well maintained perimeter barriers (fences, walls, railings, etc.), will mitigate against cargo crimes and the illegal entry of contraband merchandise or unauthorized persons into the United States.

Physical security of ports and terminals is essential to protect the integrity of the seaports. But there is another aspect of seaport security that is of critical importance to the security of the nation, and that is the custodial and informational control over the cargo, passengers, and crewmembers that enter and leave the country through its seaports.

The U.S. volume of trade in imports and exports represents 20 percent of the world's economy. Against this unending flood of manufactured goods, raw materials, and agricultural products are arrayed the various federal regulatory and inspection agencies that are tasked with protecting the country from harmful imports and our national interest from the export of restricted goods. Further complicating that responsibility are criminal enterprises and terrorist organizations that exploit the complexities of international trade and transportation for their illicit activities. In fact,

terrorism, serious crime and inadequate cargo control are the most obvious threat vectors in seaports today.

Customs was created in 1789 with the mission of examining every vessel and all merchandise entering the United States to ensure that applicable duty was paid and that the import transaction was in compliance with all laws. Customs still has this function today, in conjunction with other agencies and departments, but the law does not require, nor can it be expected, that Customs will inspect each piece of merchandise entering the country. Today, much of the routine work is accomplished through electronic data processing, and the inspectional activity is governed through risk management systems. To provide some perspective, a profile of the international trade environment is provided below:

- More than 600 laws and 500 trade agreements are enforced on import transactions.
- All import cargo has to be classified in one of the 20,000 categories of the international Harmonized Tariff Schedule. This classification is the key to determining admissibility, duty rates, and other import requirements.
- More than $22 billion in duties is collected annually on imports.
- The United States has 301 ports of entry where merchandise can legally enter or exit.
- Revisions to provisions of the trade system occur frequently.
- Cargo is processed 24 hours a day, 7 days a week.
- Some 100 million trade transactions take place every year, ranging in size from merchandise carried by passengers to shipments worth hundreds of millions of dollars.

The requirements for admitting international cargo into the country are set forth in Title 19 of the Code of Federal Regulations, and the complexity of this process should not be understated. There are 60 federal agencies that have an interest in international cargo. A few examples of the diversified agency interests are listed below:

- Dairy products, fresh fruit, vegetables, plants, nuts, live animals, meat products, poultry, bees, and honey are some of the imports that are of interest to the Agriculture Department (Food Safety Inspection Service, Animal and Plant Health Inspection Service, Plant Protection and Quarantine), Food and Drug Administration, and the Fish and Wildlife Service. Arms, ammunition, and radiological materials are subject to restrictions by the Bureau of Alcohol, Tobacco, and Firearms, the Office of Defense Trade Controls, the Department of State, the Department of Commerce, and the Nuclear Regulatory Commission.
- Consumer goods, electronic products, and energy conservation products are subject to restrictions by the Department of Energy and the Federal Trade Commission.
- Foods, drugs (including narcotic derivatives), cosmetics, and medical devices are subject to requirements of the Food and Drug Administration, the Drug Enforcement Agency, the Department of Agriculture, and the Public Health Service.
- Textiles are subject to requirements of the Federal Trade Commission, the Department of Agriculture, the Customs Service and the Commerce Department.
- Alcoholic beverages and tobacco products are subject to requirements of the Bureau of Alcohol, Tobacco, and Firearms, the Animal and Plant Health Inspection Service, the Food and Drug Administration, the Customs Service, and the Internal Revenue Service.

These are only a representative sample of the tens of thousands of product categories that are imported into or exported from the United States every day.

Of all the federal agencies sharing an interest in cargo control, Customs is the one agency that is staffed at every port where imports or exports occur. Customs has the responsibility to enforce all of the laws and trade agreements that pertain to cargo, in addition to mission fulfillment when other agencies are not present. Of the inspection agencies, Customs has the largest presence at seaports; the Department of Agriculture, through its Animal Plant Health Inspection Service and Food Safety Inspection Service, is the second largest force. The Food and Drug Administration also has inspectors near some seaports, although in lesser numbers.

In conducting their inspection efforts, federal inspectors are under increasing pressure to expedite their work. For example, one ocean container is landed in the Ports of Los Angeles and Long Beach every 20 seconds. In other words, upwards of 240,000 pounds of cargo landed every minute in 1999 just in Los Angeles and Long Beach.

The pressure to meet commercial sector just-in-time inventory requirements and the necessity to move the containers to prevent seaport terminal congestion, have created an environment in which there is little time or ability to examine international cargo. Less than 2 percent of import and 1 percent of export cargo is physically inspected before release. That is why the federal inspection agencies increasingly rely on selective targeting techniques and electronic data processing

In addition to the commercial pressure to clear import cargo, serious crime threats and the potential for terrorism are associated with international commerce. There is also an entire array of health, safety, fraud and environmental threats, including drug trafficking and other smuggling in cargo arriving from foreign countries. The monitoring of all imports and exports to ensure their compliance with U.S. laws and regulations is difficult when the multitude of requirements and the rapid service that business expects are factored together.

The convergence of threat vectors noted above can best be addressed through better coordination among the multiple federal agencies that have jurisdictional and/or regulatory interest in the seaport environment. In ports where there are shared facilities, interagency coordination is advanced, and if the shared inspection facility is situated directly on the ocean terminal property, cargo control is enhanced.

Federal officials must also accomplish their mission objectives without creating undue delays in the movement of legitimate cargo. One of the keys to managing this challenging environment is the use of automated information processing systems and applied technology such as high energy X-ray container scanners and mobile computer systems to bring on-line access into the most remote cargo or passenger examination stations.

Electronic System for Processing Imports and Detecting Violations

In 1984, Customs implemented the Automated Commercial System, which allows importers to file import documentation and pay duties electronically. Although 99 percent of the formal entry documentation is filed through this system, this represents only a portion of the information that federal officials need to carry out their responsibilities. For example, formal entries represent but a portion of the cargo that actually arrives on a vessel. In this section we describe how the formal entry system works and identify the cargo that arrives and is not immediately covered by this system.

The Automated Commercial System was designed to process import entry data, calculate duty, use tariff classifications to

identify shipments of interest to federal agencies, receive manifest data (bills of lading), and find routine errors in import data. The violation histories compiled provide excellent data not only on the shipper, importer, and consignee, but also on the commodity. With this information, federal officials can identify frequent violators and the commodities that are most likely to incur cargo and entry violations.

Random sampling was added to the Customs network several years ago to ensure that routine, low-risk shipments were not automatically bypassed. The random sample selections are computer-generated and are also useful to assay the flow of imports for overall regulatory compliance. Predicated upon the compliance rate, revenue implications such as duty and tax losses may be derived. Overall, this profiling provides a more focused view of the import cargo picture and where resources are best spent.

The Customs Service coupled the complex criteria screening with routine entry and manifest data processing in a way that frees officials from rote document handling so that they may concentrate on detecting violations and apprehending violators. Systems that use artificial intelligence and more complex screening systems are under development.

It is the detecting of any discrepancy that can lead to identifying violations, serious or not. To the extent that this process can be performed electronically, it is generally quicker and more reliable. About 90 percent of the ocean manifests are filed electronically via the automated manifest system (AMS) and 98 percent of all import entry transactions are filed electronically via the automated broker interface module of the Automated Commercial System network.

The vessel manifest is an important tool for monitoring international trade. A manifest is a list of all cargo that has been taken aboard the vessel, the ports where the cargo was loaded, and the ports where the cargo is slated for unlading. The manifest also provides fundamental shipment information consisting of the commercial parties (shipper, consignee, and notify party), cargo description, marks and numbers appearing on the cargo, the serial number of the ocean container that it is stowed within, special handling information, stowage locations in the vessel, and hazardous cargo data. Literally since the beginning of recorded history, a manifest of goods has been deemed essential in the regulation of trade and the control of cargo.

Only about 50 percent of the cargo that arrives by vessel in the United States becomes an official import, with the detailed information required, at the first port of arrival. For example, some cargo arrives in the United States on the West Coast and travels by land to Mexico or Canada, or to an East Coast port for export by vessel to Europe. Other import cargo is immediately sent to a foreign trade zone, a bonded warehouse, or a container freight station before entry requirements are satisfied.

Another provision of the Customs regulations, called "in-bond," allows cargo to be transported from the port of arrival to another U.S. port for formal entry into the commerce or for loading onto a vessel for export to a foreign country, without the payment of duty or taxes. For example, cargo may arrive by vessel in Tacoma and be transported by truck to Cincinnati. The transportation to Cincinnati would be authorized after the importer, its agent, or the importing carrier filed only minimal information about what the cargo contained and pledged to be liable for any duty and taxes that might accrue if the cargo were misdelivered. Formal entry requirements would be satisfied in Cincinnati.

Another concern relates to "consolidated shipments." When shipments are not

large enough to occupy an entire ocean container, several shipments are combined to fill one container. Generally, the container contents are manifested as "various" or "assorted," by the foreign freight forwarder, providing federal inspectors with no useful shipment information.

Therefore, the 50 percent of the cargo that does not become an official import at the port of arrival poses the largest risk. The information requirements for these shipments is less than for the entry documentation. Federal officials do not receive sufficient information to make admissibility decisions on this cargo.

Bridging the entry and manifest systems is the cargo selectivity application that performs automated screening of the entry data against criteria databases for the purpose of admissibility and release.

In the late 1980s, the Office of Management and Budget directed that there not be a proliferation of electronic systems in the agencies that deal with international trade. It decided that all other agencies would link into the Customs system to ensure that the private sector has only one point of contact for electronic submission of trade information. Coordination between federal agencies must not be limited to operational procedures, such as cargo examinations or vessel inspections, but must be extended to the arena of information sharing through electronic data interchange (EDI).

Predicated upon the OMB decision, the Customs information management and processing systems (Automated Commercial System, automated manifest system, automated broker interface, etc.) are of critical importance. Those systems process the electronic equivalent of millions of documents and forms that are associated with the importation, movement, and clearance of hundreds of billions of dollars of commercial cargo. These underlying systems must be strengthened to accommodate the ever-increasing demands of international trade, and it is important not only that robust electronic data processing systems are maintained, but that such systems continue to evolve and develop to reflect the changing trade environment and interagency enforcement and compliance priorities. The Automated Commercial Environment plan of the Customs Service is a step in that direction, and if the initiative proceeds, its development should be coordinated with other federal inspection agencies to ensure that their informational needs are accommodated within the $2 billion that the new system is estimated to cost.

Coordination is also needed in the operational environment to produce greater service level efficiencies and coordination is absolutely essential in the realm of electronic data processing to avoid mistakes that could cost tens of millions of dollars in misdirected development efforts.

Better Information Via Electronic Interfaces for Cargo Control

To avoid delaying the movement of legitimate cargo and to ensure regulatory compliance, federal inspection agencies need timely access to shipment information and the ability to analyze the data quickly with automated processes.

Even with automation, the practices and procedures used to track merchandise entering and leaving the country have eroded over the past decade for a number of reasons:

- The volume of trade has increased exponentially over the past 30 years, making it important that the federal government use selective targeting techniques in its inspection processes.
- The business community demands immediate release of cargo to maintain the just-in-time inventory systems and to reduce congestion at seaports; despite these demands for immediate clearance of cargo, business has been unwilling or unable to consistently provide accurate and timely information.

- Federal regulations frequently do not require accurate accounting for incoming or outgoing cargo until days or weeks after it has left the seaport.
- Carriers do not believe that they should be held responsible for an accurate accounting of the cargo that they bring into the country, arguing that it is the shipper's responsibility; carriers maintain that they have no responsibility to verify the contents of a container.
- Even if discrepancies with the carrier manifests are detected, the carriers have 60 days to correct the manifest before penalties can be assessed. If the manifest is not corrected after 60 days, the maximum penalty that inspectors may issue is $1,000 (19 USC 1584) unless the agency can prove fraud; carriers appear to treat the penalties as a cost of doing business.
- Consolidated shipments often contain no information on what is included in the container, listing cargo as "various" or "assorted merchandise."

Although the federal government does receive alternative and supplemental shipment information, there are timing issues. For example, the import entry documentation contains more information than the manifest, but the documentation is not required for at least 5 days after arrival, and complete entry summary information is not required until 10 days after release of the cargo.

How accurate are manifests? Customs reviewed 633 carrier arrivals in 38 seaports. The results indicated that 119 of the manifests, or 19 percent of the sample of 633 vessels, were discrepant. In other words, the ships carried more or fewer containers than they listed on their manifests. However, once Customs notified them of the discrepancy, all they had to do was make corrections to the manifest within the 60 days after arrival and no penalties could be assessed. That procedure is provided for in the Customs regulations.

In March 1999, Customs initiated a new vessel manifest compliance audit program. Under this program, Customs not only counts the containers on the ship, but also compares the manifest description with the contents of the cargo container. Here again, the carrier can correct inaccurate or misleading manifest descriptions within the 60-day grace period. The results for the first year are as follows:

- Of 181 ship manifests reviewed, 96 of the ships were found to have more or fewer containers on board than identified on the manifest, for a 53 percent discrepancy rate.
- Of 921 containers that were physically examined, 91, or 9.8 percent, had discrepancies, as follows:
- 28 containers (3 percent) had incorrect quantities.
- 46 containers (4.9 percent) had a description discrepancy.

17 containers (1.9 percent) lacked sufficient information. These findings are indicative of systemic problems in the trade practices, and regulatory changes are needed to improve them. However, even existing regulations are not being followed. The automated data systems were designed to reduce the need for additional resources, and they have made a major difference. However, without a way to ensure that the data supplied by the business community are accurate, the entire trade system is at risk.

Criminal Abuse of the Federal Inspection Control Systems

The lack of effective cargo control allows goods to be unlawfully manipulated or diverted into the commerce of the United States. This has significant negative economic consequences, ranging from lost duty and tax revenues to the United States,

to failure to enforce international trade agreements and restrictions on import or export cargo. In addition to the revenue implications of inadequate cargo control, the health and safety of American citizens may be jeopardized when unapproved and unsafe products are smuggled into this country or unlawfully diverted into the commerce from shipments not intended for entry into the United States.

The Commission found that inadequate cargo control facilitates criminal activity. The most flagrant examples of ineffective cargo control were found at Los Angeles/Long Beach, where several investigations revealed that more than 2,000 containers with nearly $260 million of merchandise were diverted into the commerce of the United States without federal inspection, the proper payment of duty, or compliance with international trade restrictions or agreements. The loss of revenue to the United States was more than $25 million in this one case.

This diversion scheme involved the transportation of merchandise from the Port of Los Angeles via truck to Laredo, Texas, under Customs transportation and exportation bonds. Once the merchandise arrived in Laredo and the applicable transportation and exportation bonds were accepted by Customs for the merchandise to be exported to Mexico, the merchandise was immediately and illegally delivered back to the importer's warehouse in Los Angeles or to other distribution locations. Eventually the violators did not even attempt to deliver the goods to Laredo; instead, a decoy shipment was kept in Laredo. If Customs ever wanted to examine a shipment, the decoy shipment would be presented. Over time, the decoy shipment aged to the point that the boxes were falling apart when the operation was brought to an end by Customs seizure. Seven individuals were arrested, indicted, and convicted of smuggling goods into the United States, and $4.8 million in merchandise was confiscated.

Foreign trade zones are also exploited by commercial smuggling organizations. In one scheme presented to the Commission, 200 containers of wearing apparel valued at $1.6 million were smuggled through a foreign trade zone. The violator, who was the importer of record, either sold the goods without authorization or used fraudulent transportation and exportation bonds to claim that the goods were exported to Mexico. The merchandise was never exported; it was delivered directly to buyers in New York. The loss of revenue to the U.S. government in this case was $900,000.

In another investigation, a New York-based importer caused the diversion of about 325 containers of textiles with a value in excess of $100 million from the Port of Miami. The truck driver was paid $500 for each container delivered to New York and the broker was paid $13,000 for false documents per container, adding up to a total of about $2.3 million over 18 months.

Inadequate cargo control can implicate concerns beyond duty or tax revenues. Inadequate cargo control can threaten the health and safety of the American public. An example of this type of violation was the importation of tainted swordfish from South America.

Generally, the Food and Drug Administration identifies swordfish for automatic detention because it must be tested for mercury content. In cases where excess mercury levels are detected, regulations require that the products be destroyed or exported under Customs supervision. To avoid the automatic detention, importers either change the country of origin or falsify the description of the shipments. In some cases, importers simply fail to deliver the swordfish to the Food and Drug Administration testing site. In cases where excessive mercury levels are detected, importers may substitute the shipments,

not export them at all, or import them again through other seaports.

Another vector for dangerous goods to enter the U.S. commerce is for cargo to be smuggled through Puerto Rico to the mainland United States. To counter this threat, the Food and Drug Administration has formed a partnership with the Puerto Rico Hacienda Police as a means of generating referrals because of the high volume of container cargo that the Hacienda Police inspect in the process of assessing a local tax.

To understand the scope of this problem, consider that an estimated 45 percent of smuggled unapproved medical devices manufactured in foreign countries under unknown conditions travel through Puerto Rico and ultimately arrive in the United States.

Exploitation of Current Control Systems

As previously noted, upwards of 50 percent of imported cargo is not cleared at the first U.S. port of arrival. The unentered cargo is moved in-bond to another U.S. port for consumption entry or export from the country. Unfortunately, as implemented, the in-bond procedures of the U.S. Customs Service deny the federal government detailed information on cargo that is transiting the United States.

A portion of the cargo arrives that at West Coast ports via ocean carriers from Asia, travels across the country by truck, and exits East Coast ports for transport to Europe. In these instances, the provisions of in-bond are used as a convenience to shippers and importers outside the United States. Metaphorically, that aspect of the in-bond procedures renders the United States the doormat of world commerce; we facilitate international trade and get stuck with the dirt of illegal diversions, contraband, and revenue loss.

In addition to the export bound foreign cargo transiting the United States, a far larger portion of imported cargo is transported from the first port of arrival to an in-land destination where Customs and other import formalities will be transacted. This cargo moves over domestic roads and through cities to foreign trade zones, bonded warehouses, and containerized freight stations (CFS) with very little information required from the importer before arrival of the cargo at the destination location when Customs clearance procedures will be initiated. Some federal law enforcement officials believe that criminal activity is facilitated through the loosely controlled interstate movement of imported cargo upon which no duty or tax has been collected. Once the in-bond movement begins, the importer has up to 30 days to complete the in-bond transportation and then 10 days after arrival to complete the Customs (entry filing) procedures. As a consequence, the collection of duty and tax payments is deferred. More significantly, federal law enforcement officials frequently observe that this transportation interval provides the time and the opportunity to divert or substitute cargo, evade duties, or smuggle unlawful merchandise. Customs has made unsuccessful attempts to eliminate this system.

That the in-bond system may be abused is highlighted in the following examples from major ports:

- As previously described, the in-bond procedures were used to facilitate the unauthorized diversion of 2,000 container loads of textiles, which are subject to import restraints, into the commerce of the United States without the payment of duties.
- The Customs office in a Gulf Coast port reported that in-bond cargo constituted its highest-risk category of shipment. It cited misclassification, transshipment, quota/visa fraud, and intellectual property rights violations as being present in in-bond shipments. A Northeast Customs office reported the diversion into

the U.S. commerce of millions of dollars of in-bond merchandise with no payment of duty or compliance with visa requirements.

In the Ports of Los Angeles and Long Beach, some container freight stations (CFS) are more than 30 miles from the waterfront and are visited by Customs officials on an as needed basis. The Commission was told that the interval between dispatch of an uninspected container to the CFS and the subsequent arrival of Customs inspectors to examine the goods could be one to two weeks after the container reached the CFS. During that interval, the integrity of the unexamined container could be compromised.

It is also important to note that merchandise that is subject to import restrictions or forbidden entry into the commerce of the United States is permitted to move through the United States for export to a third country. Only the integrity of the bonded carrier and the absence of criminal intervention or accidents during transportation prevent the cargo from being released into the commerce or environment of the United States with potentially adverse consequences for the economy and health of the nation.

A vital first step toward regaining control over the movement of unentered cargo would be to increase the kind and quality of data that must be in the possession of the appropriate federal agencies before imported merchandise was permitted to move beyond the first U.S. port of arrival. The level of information required on imported merchandise should be made uniform for all entries, including in-bond transportation entries, and such information should be accepted from any entity in the trade sector (carriers, importers, customs brokers, etc.). This enhanced reporting requirement should not infringe the rights granted to carriers in the Customs regulations (19 CFR 111.3) and the provision of the Harmonized Tariff System identification number for enforcement purposes should not be considered as "customs business" in statutory terms.

The transportation community should be encouraged to electronically transmit the vessel cargo information (i.e., manifest data) into the Customs Automated Commercial System before the arrival of the vessel at the U.S. port, and under no circumstances should any imported cargo be permitted to move beyond the first U.S. port of arrival, via the in-bond procedures, if the related shipment information had not been electronically transmitted to Customs.

Resistance to the enhanced informational reporting requirements, particularly if the desire to capture entry level information before in-bond movement results in the disenfranchising of the transportation party from the right to file in-bond transportation entries with Customs, may be anticipated from some sectors of the trade community.

Additional resistance to a change in in-bond informational requirements may be expected from the custodial entities such as port authorities, terminal operators, local trucking and cartage companies, and long haul motor and interstate rail carriers if the enhanced level of information-gathering leads to slower release of ocean cargo and the attendant consequence of terminal-port congestion including adverse impact on vessel rotations into and out of the port.

Importers, customs brokers, and custodial entities at in-land ports that were the destination of in-bond traffic may offer objections to any proposed changes in in-bond informational requirements if those parties perceive an adverse impact on their local revenue streams that depended on in-bond movements.

The fundamental weakness inherent in the in-bond system is the practice of allowing unexamined cargo to transit the United States. The raison d'être of in-bond, the deferral of duty and tax payments, would

not be compromised if examination, for enforcement or compliance or safety purposes, were conducted before removal from the first port of arrival.

Effect of Undetected Violations on Food Supply

Criminal activity is not limited to theft of cargo or denial of revenue to the government. Criminal threat vectors also include the for-profit importation of forbidden or unapproved foodstuffs or pharmaceuticals and the introduction of invasive organisms that harm our agriculture or environment.

U.S. agricultural interests have suffered major losses as a result of introductions of foreign insects. The Great Lakes are plagued with zebra mussels that are damaging public utilities such as power plants. The states of Florida and New York are contending with invasive blights, a citrus canker in Florida and the wood destroying Asian longhorned beetle in the Northeast. Public concerns have been raised about the safety of imported food that may be processed in countries where the health laws and sanitation standards may be far different from U.S. standards. Some examples of these problems:

- Infant powdered milk was imported into a foreign trade zone from Ireland and Holland without the FDA-required lot numbers or manufacturing codes. In addition, the manufacturer was not registered with the FDA as required. While the milk was in the foreign trade zone, the importer removed the label with the lot codes from the cans. The cans were sold to U.S. companies and relabeled for U.S. consumption. The FDA sampled the powdered milk from a dealer's warehouse and confirmed the cans were produced by foreign manufacturers without adequate quality control procedures. On February 26, 2000, the importer plead guilty to a felony count (18 USC 2320) for trafficking in infant formula that was packed in counterfeit labels.
- In July 1999 an importing firm and a freight forwarder were fined $650,000 for the mislabeling of $6 million worth of swordfish over a 12-month period. Under FDA regulations, unless the foreign seafood processor is exempt, all importations of swordfish must be tested to verify that mercury residues are within permissible levels.
- Since 1990, brined and canned mushrooms from the People's Republic of China have not been allowed entry into the United States because of staphylococcal entertoxin contamination. Shipments may only be released into the United States on a lot-by-lot basis after the FDA is satisfied that the product is compliant. Since the ban was imposed, 12 significant seizures of Chinese mushrooms labeled with misleading country of origin (Taiwan, Indonesia, Thailand) or falsely invoiced to hide the true processor in China (the invoiced manufacturer did not match the product code on the end of can) have been made.
- Decomposing shrimp (Food and Drug Administration levels 2 and 3) shipped from an unapproved foreign packer were imported into South Florida. The shrimp were defrosted and then washed in a bath of chlorine, copper sulfate, and lemon juice. Repacked and refrozen, the product was sold as "fresh-frozen" in Florida and Virginia. Five company executives were indicted in the scheme, which involved imports from China and India.

Exotic forest pests (insects) or pathogens (diseases) have been released into the environment from imported merchandise or from the solid wood packing material that contained imported merchandise. The recent discovery of the Asian longhorned beetle has already cost New York City $5 million for tree removal. The state of Illinois removed 20 square miles of forest in an attempt to halt the spread of the beetle. The Department of Agriculture estimates that at risk are 279 million acres

of hardwood stands and fruit orchards in the eastern United States. Potential economic losses (timber, fruit, syrup, tourism) could reach $41 billion annually if the beetle is not contained.

Inadequate or missing information on a vessel manifest could result in a contaminated shipment being overlooked, with the consequent introduction of an ecologically or economically harmful pest. The Department of Agriculture identified the following pests and pathogens as having been introduced into this country from imported cargo or its packing materials: Asian longhorned beetle, pine shoot beetle, gypsy moth, chestnut blight, Dutch elm disease, and Japanese cedar beetle.

Consistently, the federal agencies that were interviewed complained about the accuracy and completeness of shipment information. In ports we visited, import vessel manifests had been presented with some of the cargo described simply as "merchandise," or "assorted." Similar findings were reported at the other survey ports.

Need for Inspectors on the Docks

Regardless of agency, the inspector's work frequently involves more sitting or standing behind a computer terminal than actually doing on-site inspections of cargo or passengers. Collaterally, this has changed the way business is conducted on the waterfront. Customs, for example, has moved most of its commercial inspections off the port grounds, to examination stations that are often miles away from the seaport.

More than a decade ago, Customs developed the "central examination stations" that are generally located on private sector rented premises. Businesses are permitted to compete for the right to operate these inspection stations and charge those whose cargo is being inspected for the service. Again, this means that the inspectors and the federal deterrent presence are not on the docks.

The absence of federal inspectors on the docks opens more opportunity for criminal activities and for criminal enterprises to take hold. Federal investigators have noted that a substantial number of their smuggling cases, especially drugs, involve internal conspiracies. In the absence of a highly visible federal presence, such conspiracies can only grow more brazen. The simple fact of a highly visible uniformed federal inspectional presence on the waterfront facilities does have a deterrent effect much as the return of uniformed policemen to the streets has a deterrent effect on street crime.

The utility of returning the federal inspection presence to the waterfront cargo environment is self-evident. The return of the federal presence could be a force multiplier if the representatives of the various agencies were co-located in shared Federal Inspection Stations located directly on the ocean terminal property. If the shared facilities are equipped with non-invasive cargo examination tools, such as high energy X-ray container scanners and unloading platforms, as the Commission members witnessed at the European Container Terminal in Rotterdam, both the government and the private sector accrue benefits from more rapid and efficient cargo control and clearance methodologies.

In every port visited, the consensus was that more federal inspectors were needed at the docks. The number of inspectors and criminal investigators has simply not kept pace with the trade volumes. Officials believe they are catching only a small percentage of the violations. At Commission forums, terminal operators and others in the custodial cargo community (truck fleet operators, railyard security personnel, etc.) said they would welcome the return of the federal presence to the waterfront.

Additional inspectors and criminal investigators at seaports would appreciably assist in handling the increasing trade vol-

ume, and there are other things that can be done. One example is mobile computer systems that can provide the inspectors and criminal investigators with more and timely information and free them from being tied to their office computer terminals. Many police forces now have computer technology in their cars, where it can be secured and the officers can be mobile.

In summary, if the Federal Inspection Stations were located at the docks (on the container terminal itself) rather than in remote private sector locations away from the ports, the commercial parties (carriers, importers, brokers) would benefit from speedier cargo exams. It would also be possible to coordinate cargo examinations among the various agencies. The federal agencies would then be able to share equipment, reduce costs, and coordinate enforcement and compliance examinations. Shared facilities equipped with high energy X-ray devices would benefit all federal inspection agencies and their partners in international trade.

Such a redeployment within the port (not necessarily requiring additional staff) and a technology upgrade effort could be done in conjunction with a five year technology development plan (discussed in Appendix E) that would encompass the needs of all federal inspection agencies from the perspective of technology requirements, cargo examination facilities, and office space for the inspectors and information analysts.

Export Cargo Control

Historically, the export transaction has drawn less scrutiny from the federal inspection agencies than the import cargo that is a both source of revenue and a vector for contraband. The products of our factories and farms are joined with the mass of international cargo that is flowing through our intermodal transportation network en route from one corner of the world to another. Collectively, this mass of domestic and foreign goods is the export cargo of the United States. In 1998, the United States exported 366,016,833 metric tons of goods by water.

It is important to note that although export transactions are conceptually the same as the import process described above, exports have an entirely different legal framework. The regulations and procedures for imports are very different from those for exports.

In the export arena, two federal agencies have preeminent roles: Customs and the Department of Commerce. Customs has inspectors at the seaports that review documentation and conduct inspections of export merchandise, and Customs special agents conduct criminal investigations of violations of all export control laws, including strategic dual-use goods and technologies, defense articles and services, and economic sanctions and embargoes. Commerce is the principal recipient of the information that is collected on exports after the cargo leaves the port. It contains a federal law enforcement agency dedicated solely to export enforcement. In addition to Customs and the various departments within Commerce that are concerned with exports, a number of federal agencies have licensing oversight, including the Department of State's Office of Defense Trade Controls and the Department of Defense's Defense Threat Reduction Agency. Others, such as the Food and Drug Administration and Agriculture, are monitoring the export of restricted or forbidden imports.

The laws and regulations governing exports cover a broad scope. They deal with everything from licensing dual-use items and munitions to ensuring that only safe agricultural products are exported to other countries. Two primary export documents that enforcement agencies use are the shipper's export declaration (SED) and the shipper's manifest. Except in specific cases, shipper's export declarations may be

filed up to four days after the ship departs the port. The specific exceptions, in which documentation must be filed with Customs in advance of the ship's departure, include the following:

- The currency and foreign transactions reporting requirements are set forth within Title 31 of the U.S. Code. For all currency shipments valued at $10,000 or more, a Customs Form 4790 must be presented to Customs before or at the time of export.
- Munitions and weapons: Department of State licenses (DSP-1, 5, 73, 83, 85, 94 as appropriate) and/or the Alcohol, Tobacco, and Firearms (ATF Form 9) must accompany the export shipment of certain classes of munitions and other defense articles.
- Chemicals used in illegal narcotic production ("pre-cursor chemicals"):
- Critical technology, nuclear nonproliferation items, embargo enforcement and national security issues: Export of qualifying goods requires that shipments of such articles or technology be licensed for export and that the license be verified prior to actual exportation.
- Used motor vehicles: Customs Regulations (19 CFR 192.2) require the presentation of documentation three days before the exportation of the vehicle.

Thus, exports that include articles covered in these areas must present documentation before the ship leaves the seaport. The obvious problem with this framework is that it is unlikely that someone attempting to smuggle goods out of the country without proper clearances would stop to file the appropriate paperwork. Thus, serious enforcement efforts can begin only after the cargo has already left the seaport. In addition, after the ship leaves the port, federal inspectors cannot verify whether the paperwork was accurate. Federal enforcement officials are frustrated with the general process.

Another current practice, delayed filing privilege, is at the center of the problem of export control, and it defines the fundamental difference between the import and export cargo control environments. Export reporting is on an exception basis, while for imports all shipments are reported to the federal authorities before or at arrival. Enforcement personnel believe the delayed filing compromises the mission of export control for all meaningful purposes.

In addition to its own concerns, Customs assists a number of agencies to enforce their export control regulations along the U.S. borders. Principal among those are the Department of Commerce, the State Department, the Bureau of Alcohol, Tobacco and Firearms and the Department of Energy.

Illicit shipments are more likely to be concealed within or falsely described under a non-controlled category. That is why it is essential that export information filing before vessel departure be made mandatory for all merchandise, not just the sensitive categories noted above. The control of export cargo effectively ends when the cargo is laded aboard the vessel. Although exported cargo, upon demand, can be redelivered to the United States, there is no guarantee that what is returned is in fact the same merchandise or all of the merchandise that was originally exported.

Information-processing and document analysis are parts of a risk assessment criteria screen through which suspect shipments can be assessed. However, if the export shipment information is not available, by established business and regulatory practice, up to 4 days after sailing of the export cargo, there is no chance of performing pre-export risk analysis on the vast majority of export cargo transaction.

The most compelling reason to be concerned about exports is the illegal exportation of sensitive technology and goods. This is an issue of national security. We know from intelligence sources that U.S.

products are being aggressively sought by terrorists, rogue states, narco-traffickers, and others. The law enforcement community informs us that these goods are being exported through our seaports, in addition to airports and land borders. Interviews conducted at the 12 seaports surveyed confirmed this to be the case.

Based on law enforcement investigations and interviews conducted at the 12 seaports surveyed, we know that seaports are vulnerable to those trying to acquire or sell U.S. goods illegally. Another reason criminals are able to smuggle is that it is relatively easy to circumvent required export document requirements. Information given by exporters on paperwork is often vague, inaccurate, or missing completely. For example, at one of the ports we visited, authorities noted that the largest export commodity from the port is described as "general cargo." At another seaport, we were told that some major shipping lines are flagrant violators, having manifest accuracy rates of only 40 percent. Another official stated that the submitted forms are often illegible. Customs does conduct post-audits (often months after the ship leaves the port) of manifests and shipper's export declarations at the 12 seaports surveyed, but at rates that range from less than 1 percent to 10 percent of all manifests.

Customs estimates that less than 1 percent of U.S. exports are inspected. Law enforcement officials interviewed at ports believe that illegal shipments are likely to pass through the system undetected. One way to improve the federal ability to inspect and monitor the increasing amounts of export cargo is to tighten the regulations governing the information provided by exporters and their agents. Currently, most shipper's export declarations and on-board bills of lading are prepared by the exporter or its agent, the freight forwarder. These documents are received and collated by the vessel operator at its offices or by its agent (the receiving clerk) at the terminal location. These practices reflect a pre-automation hard copy inventory control system and must be revised to benefit from and better manage the electronic commerce environment of today's shipping industry.

Although national security ranks on top of the list for risks, an inadequate export control system affects other interests, too. The Food and Drug Administration has identified export fraud as a major area of concern with serious economic and health implications. Legitimate products purchased at steep discounts for export are secretly diverted into the domestic commerce and false export declarations are issued to cover the diversion. The American producers are deprived of lawful revenue and the U.S. consumer is put at risk in the event of a product recall because there is no legitimate record of these diverted products in the U.S. marketplace. (There is also export fraud associated with the diversion into the U.S. commerce of rejected foodstuffs and that issue is addressed later in this section.)

Import restrictions and export promotion methodologies, such as "Customs drawback" (refunds of previously paid Customs duties upon export of duty paid goods) have been compromised via export fraud associated with violations of the provisions of Chapter 9802 of the U.S. tariff code. This section provides for duty-free re-entry of goods that have been "advanced or improved abroad." The presentation of false export documentation is used to fraudulently enter goods duty-free that do not qualify for 9802 treatment.

Stolen vehicles have been detected in export containers in all of the 12 seaports surveyed by the Commission. In some ports, stolen vehicles concealed in export containers are a major source of revenue for domestic and international criminal enterprises. The U.S. insurance industry places great emphasis upon the detection and reduction in car thefts. Car thefts are not always victimless crimes. Crimes against personal property can be traumatic

and even deadly in some cases. The export of stolen vehicles is a major product of criminal enterprises to be found at seaports.

Exporters and outbound vessels are required by law to file accurate export information, but for decades these laws have not been enforced. Law enforcement officials interviewed at the ports believe that there is a lack of manpower and technology to enforce these regulations. In addition, efforts to gain compliance by federal officials have not always been warmly received by the private sector. Although there are complaints about the practicality of providing timely and accurate information, the state of technology has improved dramatically over the last decade. Most records, today, are automated.

The exporters, freight forwarders, customs brokers, and transportation providers that are party to an export transaction are automated within their industry sectors. Some of these parties exchange shipment information via electronic data interchange to facilitate the export transaction. Therefore, it is not unreasonable to expect them to satisfy federal reporting requirements using the Automated Export System of the Commerce Department and Customs. However, this has not been the case.

The exporter or its agent, the freight forwarder, has in its possession the shipment information before export. They should know who the foreign buyer (importer) is in order to prepare the export bill of lading. The freight forwarder should know the identity of the U.S. shipper and the foreign importer, and the description of the goods, in order to prepare the shipper's export declaration. The export carrier should know the nature and character of the goods in order to prepare a stowage plan. This information is known to the export community and should be provided to the federal inspection agencies responsible for the administration and enforcement of the export laws.

If the export control regulations of the United States are to have any real significance, the federal inspection and investigative agencies responsible for the administration and enforcement of the export regulations must know the true nature of the export merchandise, and the true identities of the shipper and end user. To accomplish this would require that the export information be available to the federal authorities in advance of the departure of the vessel.

The verification of pre-departure filing of export documentation (shipper's export declarations and the outbound export manifest) and the physical inspection of suspect shipments are the means by which export violations will be detected and prevented. Law enforcement officials interviewed at the ports believe that additional personnel devoted to export documentation review would strengthen efforts to detect illicit shipments. They also believe that interdiction efforts would be enhanced through the use of applied technology such as X-rays and computer software applications that can screen export data in advance of the vessel departure.

Benefits and Limitations of Automated Export System

Customs and Commerce developed an automated system, the Automated Export System, for the collection of export information. Until recently, participation in the Automated Export System was totally voluntary. At the seaports surveyed, participation rates varied between 1 and 6.7 percent of exports.

Its designers envision that the automated export system will improve the quality of the information that is gathered on exports by requiring that specific information be submitted for each field. The submission will not be accepted with missing or insufficient information, as often happens in the paperbound system. A beneficial consequence of the improved information will be

more reliable trade statistics and an enhanced enforcement and compliance environment for the federal inspection agencies. Furthermore, it will replace an earlier automated initiative of Commerce that allowed for the monthly filing of export information on magnetic tapes under the Automated Export Reporting Program.

The monthly Automated Export Reporting Program filing procedure removed the administrative burden of hard copy document handling for exporters. However, it also removed an important enforcement tool, which was the review and screening of the hard copy documents by the Customs Service before the transmittal of the documents to the Commerce Department (specifically, the Foreign Trade Division of the Bureau of the Census). Therefore, the first automated initiative in the export arena was counterproductive from an enforcement and compliance perspective.

The advent of the automated export system is a step in the right direction, but it has some significant drawbacks. Jointly designed by Customs and Commerce, it accommodates the informational reporting requirements of the Census Bureau and the enforcement concerns of Customs, Commerce, and other federal inspection agencies. When implemented fully, it will contain information on the shipper's export declaration, the shipper's outbound manifest, and the bill of lading for individual shipments. Currently, only the shipper's export declaration portion of Automated Export System is fully functioning.

The ability to file the shipper's outbound manifest is expected to be available in the near future. It is now being tested on a limited basis. The final segment envisioned is submission of the bill of lading for all shipments electronically. It is in the early stages of development and will require time and funding to become fully operational. When all three segments are finally implemented, the Automated Export System has the potential to be a powerful tool for targeting and enforcement purposes. The system should also enhance the reliability of trade statistics.

Despite the positive potential of having a fully functioning electronic filing system, the Automated Export System has several significant problems. One is that the filing requirements cover only certain export goods.

Under the Proliferation Prevention Enhancement Act of 1999, in the near future, exporters that are required to file a shipper's export declaration will file such declarations through the Automated Export System with respect to exports of items on the U.S. Munitions List or the Commerce Control List. This requirement is a positive change, but even more comprehensive requirements for filing are needed. If only certain licensable goods are covered, violators could simply file fraudulent paper documents that they know may receive less immediate scrutiny than the electronic filings, in order to mask their illegal exports.

For enforcement purposes, it is more useful to eventually require that all shipper's export declarations and, when a viable system is in place, all other export documentation, be filed through an automated system. The ability to cross-check all electronic submissions for a single export will allow for better targeting of suspect shipments than could be accomplished with paper submissions. Instead of slowing commerce, this should in fact speed processing and release of legitimate exports.

Timeliness is also a problem in the way the Automated Export System is currently planned. In fact, the current four-day filing of shipper's export declarations in the paperbound system may actually be better than the possible 10-day filing—even though automated—that will shortly be implemented for licensed goods. The proposed new Automated Export System filing options will hamper the use of this export information for enforcement purposes. Exporters or their agents will poten-

tially have three options for electronically filing shipper's export declarations for licensed commodities. The individual licensing agency will determine which option or options will be available to the exporter. The first option is the pre-departure submission of all Automated Export System data. This is the only option that has positive benefits for inspection and enforcement activities. The second option is the partial predeparture submission of some specified data, with the rest of the information due 10 days after export. The third option is that no shipper's export declaration information is due until 10 days after export. Some licensing agencies have already said they are in favor of an "exporter-friendly" policy of allowing the third option—for the majority of exports, submissions will not be due for 10 days after export.

Thus, while the Automated Export System may improve the accuracy of the export information, if the shipper's export declaration information is not received until 10 days after the vessel has sailed, the chance of retrieving a forbidden or restricted export is severely diminished. In fact, vessels sailing to Central or South America, where the restricted cargoes could be transferred to other carriers for reshipment to forbidden destinations in third countries, would have arrived at its destination before the documentation was even presented to U.S. authorities. Although Customs has the authority to demand redelivery of a cargo whose legitimacy is in question, if it has reached its destination there is no guarantee that what is returned is actually what was initially exported from the United States. Enforcement will lose one of the greatest potential benefits of an automated system if filing of all export documentation is not required before vessel departure.

Insufficient Export Penalties

Noncompliance with export cargo documentation requirements carries minimal consequences. Documentation violations appear regularly. In Charleston, manifest penalties averaged 87 per month. In New York/New Jersey, we were told that 2,086 shipper's export declaration discrepancies were found between January 1997 and June 1998. Some federal inspectors at various ports said they often did not pursue these violations, or if they did pursue them they preferred to issue verbal warnings.

The fines are too low to be an incentive to exporters to submit their documentation on time. Present regulations and operational policy allow for the presentation of the shipper's export declaration to federal authorities up to four days after departure of the vessel. Failure to present the required documentation on a timely basis may be sanctioned with civil penalties accruing at the rate of $50 on the first delinquent day and increasing to $100 after 3 days for a possible maximum fine of $1,000 at 12 days. However, it is the practice in many ports to wait an additional six days beyond the four-day delayed filing period before any penalty action is initiated. Obviously, this permissive environment does not promote compliance. However, because of the low level of the penalty, costs to process the penalty are more than is collected, if the violator pays.

Because the shipping industry is a very competitive environment, and the speed of delivery is a hallmark of service, the possibility of a $500 fine for late filing of export declarations may actually be viewed as an acceptable cost of doing business.

As noted earlier, the Automated Export System has the potential to make the export information available for review by the federal inspection agencies even before the loading of the vessel, if current filing requirements are changed. That would be a quantum improvement over the current practice of waiting until the hard copy document shuffle is completed among the forwarders, terminal operators, and steamship company agents, which can take up to 10 days after the export event.

For the reasons articulated above, the agencies with export enforcement tasks should review and update the appropriate sections of the Code of Federal Regulations or if required, the U.S. Code (statutory law), so that the assessment levels of fines and penalties (administrative and civil) for export documentation violations are substantially increased. To promote compliance with export regulations, consideration should be given to authorization of "on-the-spot" assessments of financial penalties for export documentation violations.

Lack of Historical or Current Statistics on Export Violations

As discussed in Chapter 3, crime statistics are not effectively collected. It is difficult to evaluate the extent of the problem or the cost to the United States of goods being illegally exported through our seaports. Few statistics capture export crime because there are no statistical reporting requirements on export-related violations or crimes involving the seaports.

Even the export-related information that is collected is difficult to retrieve from agency databases, as Chapter 3 documents. Nine of the 12 seaports surveyed do not track the accuracy rates of the Automated Export System. Only four of the 12 were able even to provide information on the volume of licensable commodities traveling through their ports.

Officials who were interviewed did express concern about illegal exports. The concerns mentioned included currency smuggling, arms trafficking, and the illegal export of high-technology military equipment, precursor chemicals, and weapons of mass destruction (WMD) technology. For example, New York/New Jersey said it had found significant illegal activity during inspections of outbound cargo. In one case, it found $11 million in currency concealed in truck inner tubes.

These concerns are corroborated by information available from the intelligence community and federal agencies. Various intelligence reports indicate that U.S. products are being aggressively sought by WMD proliferators, arms dealers, narcotraffickers, and others outside of the country. Highly sought-after items include dual-use goods such as high-performance computers and advanced electronic components that can be used to manufacture weapons of mass destruction, as well as goods that can generate income on "black" and "gray" markets, such as guns, alcohol, and tobacco.

Recent criminal cases also demonstrate that seaports are being used in these illegal efforts. One investigation by the Commerce Department's Office of Export Enforcement revealed that an American company exported potassium fluoride and sodium fluoride to Jamaica and Suriname on 50 separate occasions without obtaining the required export licenses. Potassium fluoride and sodium fluoride are controlled because they can be used to make chemical weapons. The company made false statements on export control documents in the case of each shipment. A civil penalty of $750,000 was assessed on the company. This case is particularly interesting because it was a shipper's export declaration review program in the Office of Export Analysis that led to the investigation. It demonstrates how important export documentation review is to enforcement, and how timely and complete submissions of information by exporters aids this enforcement effort.

Government export document review (export control) programs that are enforcement-oriented should be encouraged.

Food Safety Concerns Affecting Exports

Cases that involve the possible proliferation of weapons of mass destruction stand out among export cases. But there are other issues of concern, such as public health and safety. In conjunction with the export transaction, federal agencies such as Agriculture and the Food and Drug

Administration are required to provide inspections and issue certificates attesting to the fact that the export-bound cargo meets the import requirements of the country of destination. Some federal agencies also allow for the export of goods that have been refused admission into the United States. Interestingly, most agencies reported that they did not conduct inspections to verify whether the same material that was certified for export or refused entry into the United States was actually exported from the United States. In some cases, the verification of export task was deferred to Customs, which did not finally learn of the nature of the exported goods until four days after vessel departure.

Customs and the Food and Drug Administration reported significant numbers of violations involving the diversion of foodstuffs that had been denied entry into the country. Noncompliant products that were refused entry, including seafood, fruit juices, mushrooms, and products intended for specific ethnic markets, were frequently diverted into U.S. commerce. The diversion of dangerous, poisonous, or noncompliant foodstuffs into the U.S. marketplace threatens both public health and the business of the legitimate importer. These are some typical examples of these low-visibility violations that carry high-risk health and safety consequences:

- A shipment of more than 100 cartons of dried grouper fish was refused entry into the country, and the importer was granted permission to export the fish. During a spot check by a Customs inspector before export, samples of the export-bound fish were drawn and sent to the Food and Drug Administration. Analysis revealed that the product was not the original grouper, but a less expensive fish (croaker). The importer had willfully diverted the rejected grouper into the U.S. marketplace. The importer was fined $32,484.
- In another FDA case, 170 cartons of dried mushrooms were refused entry. Again, only the intervention by a Customs outbound inspection team resulted in an inspection, which revealed that the cargo being exported had, in fact, been substituted for the nonconforming and forbidden product. Physical inspection of the cargo revealed that the bag weights differed from the import documentation, that the descriptions on the cartons had been altered, and that the actual product was larger in dimension than the original import lot. The shipment was seized, and a fine of $22,066 was assessed.
- Export fraud can also involve American products. A U.S.-based exporter devised a complicated scheme that ultimately defrauded 39 companies. These violations eventually led to a prison sentence and a $1.9 million fine in 1995. The New Jersey U.S. Attorney's Office revealed that the scheme involving the legitimately discounted purchase of U.S.-manufactured products for export. Some of these products were exported and then immediately reimported under the Customs "American goods returned" provisions, which allow for the duty-free entry of American-origin goods. These reimported goods were then illegally sold into the U.S. market, without the knowledge or permission of the manufacturer, and undercutting the manufacturer's own domestic product line.
- In other cases involving U.S. goods, there was no physical exportation, but fraudulent shipping documents, including bills of lading, were produced to make it appear that the goods had been shipped overseas. The difference between the domestic and discounted export prices, which could range upwards of 50 percent, provided the profit motive for these export diversion schemes. In addition to monetary loss, the export diversion schemes caused some U.S. manufacturers to violate the

Food and Drug Administration record-keeping requirements, which could have led to serious health and safety consequences if any of the products had been subject to a recall. Also, some manufacturers received rebates from Customs (under its drawback program) and Agriculture (which subsidized sugar at below-U.S.-market price) predicated on the fact that these companies believed their goods had been exported. Among the U.S. companies or domestic affiliates that were defrauded were Alpo Pet Foods, American Cyanamid-Lederle, CIBA Pharmaceuticals, Elder Pharmaceuticals, Fissions Pharmaceuticals, Forest Pharmaceuticals, Fujisawa Pharmaceuticals, General Mills, Golden Grains, Hunt & Wesson Foods, ICN Pharmaceuticals, Nestle, Procter & Gamble, Ralston-Purina, Redmond, Schwartz Pharmaceutical, Tsumora Medical, and Van Camp-Hormel.

These examples underscore the fact that product substitution and export diversions can be detected only through examination of cargo. Furthermore, the practices are widespread, they pose significant risks for the health and safety of the U.S. public, and they can have serious economic consequences for U.S.-based industries.

Falsification of export documents and physical substitution of forbidden products hurts the American polity and impugns the integrity of American business practices. The promotion of cargo control in the export environment needs to become a national priority.

Export Control Enforcement

As stated earlier, the legal frameworks for imports and exports evolved differently. Import duties funded practically the entire federal government for nearly 150 years, so import transactions have always been the subject of concerted effort. As trade has increased, concern over the smuggling of many commodities has also increased, and the number of laws affecting imports has risen to more than 600. Export controls play a much different role. They are a protective device involving U.S. national security and foreign policy concerns as well as the protection of U.S. business, knowledge, and service. The need for increased attention on export enforcement has risen with concerns about controlling the spread of weapons of mass destruction and dual-use items used for their development; smuggling of U.S. firearms to revolutionary groups and other extremists; sales of U.S. commodities to fund terrorist operations; and other activity counter to U.S. interests.

Providing more scrutiny and control on exports, in contrast, has been more controversial. Some have viewed export controls as anti-business. Still, national security concerns are raised frequently about U.S. weapons, munitions, and critical technology being provided to our enemies. And a variety of laws and regulations are in place to control such exports. Enforcement of these laws is problematic.

- At Los Angeles and Long Beach, the two busiest ports in the country, only 9 Customs inspectors and 1 supervisor were assigned to export, compared with a total of more than 100 inspectors on the inbound side. To understand the task they face, consider that 150,000 containers a month leave from those two ports. Traditionally, the inspectors working outbound have been looking for stolen vehicles because Customs inspectors are required by law to check the paperwork for each used vehicle being exported. This leaves only three inspectors for targeting munitions list and dual-use goods—and this number actually reflects a recent increase.
- At Customs, few criminal investigators are devoted solely to working export cases. For this reason, there is no exact number of agents doing export investigations nationwide. It is estimated that in 1998, out of a total of 2,789 criminal

investigator positions, the equivalent of 126 investigators, or 4.2 percent of the total, were working export cases.

- Export Enforcement at the Department of Commerce is the only agency that investigates solely export violations. It covers the nation with 105 criminal investigators. If export enforcement is a vital national interest, staffing increases for both inspection and investigation should be considered.

With such constraints, operational coordination and shared facilities in Federal Inspection Stations at waterfront locations would serve as force multipliers in an environment now functioning with limited resources.

As a first step in this direction, the Department of Commerce should develop a dedicated team at each Commerce/ Export Enforcement field office to work with Customs to target export control crimes and provide training to Customs on export control documentation as needed. Stakeholders, such as freight forwarders, should be targeted for compliance education and outreach by joint Customs and Commerce enforcement teams as needed.

Cruise Ship Passenger Control

Seaports are also the venue for cruise ship passenger activity, and every arriving commercial vessel has non-resident crew members who represent a potential threat for illegal entry into this country. This section of the chapter will examine the issues surrounding passenger and international crew control at seaports.

The Coast Guard regulations on cruise ships are meant to deter acts of terrorism. They are aimed strictly at preventing weapons and explosives from being brought aboard passenger vessels. The regulations require screening of embarking passengers, baggage, and ships' stores, but they do not address issues relating to processing of passengers and crew through Customs, Immigration, and Agriculture.

Seaport passenger volumes have climbed steadily over the past decade, principally because of the increased popularity of cruise ship vacations as opposed to a resurgence in transoceanic passage. The cruise market is particularly vibrant in the South Florida region, where passenger capacity is so tight that new and bigger ships are constantly being constructed. The passenger cruise industry is also expanding in northern waters with Alaskan itineraries and almost every east and west coast port of any size has some cruise activity, whether daily like Miami or seasonally like New Orleans, Boston, New York, Philadelphia, Baltimore, San Francisco, and Seattle.

The fact is that the burgeoning cruise ship industry is reversing a decades long decline in waterborne passenger traffic that began with the availability of jet aircraft travel in the last 1950s. Unfortunately, the swelling numbers of cruise ship passengers provide opportunities for domestic and international criminal enterprises. Narcotic smuggling by passengers or vessel crew, commercial contraband (merchandise smuggling), illegal aliens (either secreted aboard or crewmembers jumping ship), terrorist operations, and public health menaces from communicable diseases or infested agricultural goods can all be carried on-board a cruise vessel.

Each individual arriving from a foreign country must be checked by Immigration to ensure that he or she is a U.S. citizen or has the right to be in the United States. All of these individuals are also checked to determine if they are criminal aliens, if there is an outstanding warrant for their arrest, or if other information makes them suspect as having terrorist or criminal connections. If an individual appears to have a serious health condition, Immigration is required to call the Public Health Service

to ensure that no communicable diseases are involved.

The Immigration and Naturalization Service has recognized the need to improve border control and streamline inspection processes in the seaport environment. Seaport operations have not changed substantially in decades and are overdue for streamlining and modernization. At present, the Immigration inspection processes are paper-driven and labor-intensive. For similar reasons, the maritime industry desires changes in the Immigration inspection process to decrease the paperwork burden and to more efficiently process passengers. This is especially evident in the cruise line environment where passengers may undergo multiple Immigration inspections in one voyage after short visits to foreign ports of call.

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 placed far-reaching alien control and reporting responsibilities on the Immigration and Naturalization Service. These responsibilities include the development of an automated system to collect and match the arrival and departure records for all non-U.S. citizens entering and departing the United States via air, land, and sea. This is a particular challenge in the seaport environment, which does not currently have an automated method to collect crewmember arrival and departure records. The lack of an automated seaport system makes the ready access of records at a national level impossible. Furthermore, intelligence information is not routinely shared among ports of entry.

The Immigration and Naturalization Service, in an attempt to meet these challenges, seeks to design a seaport system whose purpose is to focus existing inspection resources more appropriately. The initiative also seeks to develop alternative types of inspection procedures for crew of cargo vessels that have histories of compliance with Immigration regulations.

Seaport automation will allow ports of entry to focus resources on areas with the highest immigration risks instead of the highest volume. More time can be spent on inspection activities related to people who pose a higher risk in the seaport environment.

Passenger control extends beyond immigration concerns to encompass additional threat vectors from cruise ships. In addition to Immigration, each returning cruise ship is met by representatives of Customs and Agriculture. For example, during the period of the Commission's seaport review, Customs made 754 seizures of illegal drugs from cruise ship passengers. Threats include passenger health, crew member smuggling, illegal aliens concealed aboard the ship, contraband carried by passengers, in their baggage or secreted within the vessel itself, prohibited agricultural products, and duty evasion. The many areas underscore the need for coordination between the various federal agencies.

The cruise industry is expanding dramatically, and the expansion is expected to continue. Yet, unlike airports and land borders, commercial seaports have no clearly delineated sterile areas for federal inspection stations. At airports, the federal inspection agencies have secure sterile areas for conducting their inspections where domestic passengers, visitors, and airport workers are segregated from arriving passengers. At seaports, there is also generally a lack of suitable space to detain suspects while further checking is being done.

A review of passenger security at terminals that serve cruise lines indicates a commitment to passenger control. Passenger and cargo operations are generally segregated, at least in the home ports of cruise ships, and separate terminals are designated for cruise passengers. Terminals uniformly employ private security forces, and those personnel appear to be clear as to which police unit should be notified when there is a problem. Security procedures

are, for the most part, well coordinated between terminal and vessel personnel.

One aspect of passenger control that is of concern is the system for identifying passengers reembarking at foreign ports. While cruise ships operating from U.S. ports are required by regulation to employ procedures to prevent unauthorized access, no standards are in place for identifying bona fide passengers who seek to reboard a cruise ship after spending some time ashore in a foreign port. This provides an opportunity for stowaways or others who are not registered passengers to board. Some cruise lines issue identification cards; others simply check off passenger names on the manifest. A more secure system should be encouraged.

But the security of federal inspection space is an outstanding concern. In a typical seaport, one can observe a mix of arriving and departing cruise ship passengers, vendors servicing cruise ships, and workers employed on behalf of cargo vessels engaged in foreign and domestic activities in the port. Because distinct processes within seaports are not formally separated, dockworkers and other individuals with access to ports, such as truck drivers and vendors, can mix freely in the federal clearance environment. This negates the entire federal inspection process. For example, a drug smuggler could easily pass his contraband to someone waiting at the dock. A crew member or stowaway with a communicable disease or even a suspected terrorist could bypass the federal inspection process completely.

Because areas at seaports in which federal inspections take place are not well controlled, opportunities for illegal activities increase. Because passenger terminals are not owned or administered by the federal government, passengers disembark and enter a terminal area controlled by a private security service after immigration examination or inspection is completed aboard the vessel. The area where further federal inspections take place is not sterile. The availability of a designated federal inspection site at seaports, like the sterile area in an airline terminal, would reduce risk to federal law enforcement officers by providing an area where a suspected terrorist or criminal can be detained and adequately supervised, and it would limit jurisdictional issues related to the apprehension of aliens after they disembark the vessel.

The issues are especially problematic in light of the short time frame involved. Cruise ships are generally in port less than 12 hours. Within that short time, all passengers and their baggage must be unloaded; cleaning and trash removal must take place; new supplies must be taken on; and new passengers must be boarded with their luggage. Any repairs to the vessel must also take place at this time. Some of the larger ships hold more than 2,000 passengers, and the crew-to-passenger ratio is about 1:3, which results in additional movement on and off the ship. It is logistically difficult for the federal inspectors to control who and what goes on and off the vessels under the current arrangements.

Crew Processing Control

Foreign vessels have become an emerging avenue for aliens to enter the United States illegally through organized efforts, as stowaways or as crew “jumping” (unauthorized departure with intent to remain illegally in the United States) the vessel.

On cruise ships, where the number of crewmembers is generally about one-third the number of passengers, the clearance of crew is a substantial effort. Cargo and other commercial vessels often have large numbers of crew as well. Because most vessels calling at U.S. seaports are foreign-flag vessels, most of the crew are foreign citizens. In some cases the crews are undocumented and are not allowed to enter the United States.

Although many vessel captains cooperate fully with federal authorities, occasion-

ally Immigration has difficulty obtaining an accurate list of crew. Crew frequently change as vessels travel from port to port, and some captains do not appear to maintain adequate control of their crew. The size of fines levied against cruise lines for the boarding of improperly documented crew has risen, in turn brought on by an increase in mala fide (bad faith) crew seeking entry into the United States. Ships' officers often are inadequately trained to identify bogus documents.

If Immigration forbids crew members to enter the United States, the ship's captain has the responsibility to detain them aboard the vessel. Loose security often results in detained crewmembers leaving their vessel. Immigration does not have the resources to check departing crew against manifests, thus leaving an avenue for crew jumping.

Some of the biggest concerns of federal officials are stowaways on private vessels, passengers on day cruises, and crewmembers' visas (which are issued by the Department of State). Officials commented that such visas could easily be obtained at the last port of call before the ship reaches the United States.

Stowaways present a significant problem for law enforcement agencies in Gulfport and New Orleans, and crewmembers are often involved in alien smuggling. Another problem for law enforcement agencies is document forgery. In Mayaguez, Puerto Rico, stowaways from the Dominican Republic present a significant challenge for law enforcement agencies. Immigration contacts the FBI when it believes it has a stowaway or an alien in custody who is suspected of having ties to a terrorist organization. The FBI then interviews the subject and shares information on a need-to-know basis, which will include Immigration and the Joint Terrorism Task Force.

Military Mobilization Security at Strategic Seaports

In this post-Cold War era, forward deployment of U.S. troops and equipment overseas is a less frequently utilized strategy. Consequently, in the event of a contingency, military equipment will have to travel farther in less time to the theater of operation. Because the ongoing base realignment and closure initiatives include closing several military-owned and -operated ports, U.S. commercial ports have become critical choke points of future military mobilizations. The security of commercial ports during times of military mobilization is therefore essential to the national defense.

At the request of the Military Traffic Management Command, the Maritime Administration has issued port planning orders to 13 U.S. commercial ports. The orders define the tentative arrangements to make port facilities and services available to meet anticipated defense agency requirements during a mobilization. Military mobilizations through commercial ports would occur in the midst of all regular cargo activities. Not only would this situation increase the demand for facilities, equipment and labor, it would increase the demand for security. The designated Strategic Seaports are:

Beaumont, Texas
Charleston, South Carolina
Corpus Christi, Texas
Jacksonville, Florida
Long Beach, California
Morehead City, North Carolina
New York/New Jersey
Norfolk/Newport News, Virginia
Oakland, California
San Diego, California
Savannah, Georgia
Tacoma, Washington
Wilmington, North Carolina

A key memorandum of understanding on port readiness guides the overall outload of military equipment from these Strategic Seaports. The purpose of the memorandum of understanding is to ensure the readiness of military and commercial seaports to support deployment of military personnel and cargo in the event of mobilization or national defense contingency through enhanced coordination and cooperation among the following U.S. entities:

- Maritime Administration
- Joint Forces Command
- Headquarters Forces Command
- Transportation Command
- Military Sealift Command
- Military Traffic Management Command
- Army Corps of Engineers
- Coast Guard
- Maritime Defense Zone

The memorandum of understanding on port readiness established a National Port Readiness Network Steering Group and a subordinate working group of designated representatives from the agencies listed above. The working group is tasked to:

- Coordinate contingency planning concerning military requirements for and use of strategic seaports.
- Develop initiatives supporting military preparedness at commercial seaports.
- Coordinate operational procedures and information exchange.
- Conduct joint exercises, conferences, workshops, and training to evaluate plans and procedures.

The memorandum of understanding on port readiness also directed the signatory agencies to form local port readiness committees at Strategic Seaports to develop specific geographical and functional agreements. The activities of the port determine the composition of each committee, which might represent the port authority, Customs, the FBI, Immigration, the local police department, local government agencies, and so forth.

The key federal agency mobilization responsibilities for Strategic Seaports are as follows:

- The **Coast Guard** is responsible for enforcement of federal laws and international treaties and the security of U.S. ports and waterways. This includes but is not limited to establishment and enforcement of security zones, supervision over the loading of explosives, control of all vessel traffic within the port, harbor defense, cargo segregation at facilities and aboard vessels, enforcement of all navigational safety regulations and law enforcement aboard vessels and waterfront facilities, vessel escorts, enforcement of limited access areas, aids to navigation and port safety, and administration of all bridges over navigable waterways. In addition, the Coast Guard provides search and rescue, responds to releases of oil, chemicals (including chemical weapons of mass destruction), and hazardous materials, conducts boardings and inspection of vessels, and investigates casualties.
- The **Maritime Administration** provides U.S.-flag ships and, as necessary, U.S.-owned foreign-flag ships by requisition to meet Department of Defense requirements in time of war and non-North Atlantic Treaty Organization contingencies, and acts for the United States in North Atlantic Treaty Organization shipping affairs. For use in national emergencies, it maintains the National Defense Reserve Fleet and the Ready Reserve Force. During emergencies, the Maritime Administration becomes the operating arm of the National Shipping Authority. It is responsible for coordinating the use of ships and nonmilitary ports, and it administers a program that assures allocation and priority use of

commercial port facilities. The Maritime Administration also appoints a federal port controller, who serves as the director of the local port, to act as its agent in national emergencies.

- The **Military Traffic Management Command,** an Army command that is a component of the Transportation Command, is responsible for coordinating the movement of military traffic, cargo equipment, and personnel. During mobilization, its reserve units are activated to direct the outloading of military cargo at commercial ports. The security cell of the transportation terminal battalions supervises terminal security at the port, while the port security detachment, if available, provides access control and security for military cargo. Joint Forces Command's port support activity and deploying units assist in the security operations.

Visits by the Commission to four of the 13 commercial Strategic Seaports revealed that the "National Port Readiness Network and local Port Readiness Committee" concept is fundamentally sound but in need of increased emphasis. In particular, local memorandums of understanding need to be updated, local Port Readiness Committees need to meet more often, nontabletop exercises need to be held more frequently, and resolution of unsolved issues and problems need to be escalated.

With many competing operational demands, no dedicated resources, and little guidance from the National Port Readiness Network, the local Coast Guard Captain of the Port is often forced to place this collateral duty on the back burner until an actual military mobilization arises. Adding to the problem is the fact that the national port readiness network has not made it a priority to provide for actual port readiness exercises, and therefore only tabletop exercises are held on a yearly basis. Finally, vulnerability and threat assessments are lacking in the Strategic Seaports, although the Coast Guard has done some local threat assessments.

No specific security standards have been established for facilities used by the military during mobilizations. The Army is tasked with landside security for strategic outport operations. This security, however, is centered on protection of personnel and specific cargo within allocated terminal confines and is defined in memorandums of understanding (both joint and between Military Traffic Management Command and Joint Forces Command). The overall level of landside security for the entire port is a function of local memorandums of understanding between the Army and the port authority. Depending on the strength of the local memorandum of understanding, the level of port security provided could potentially be inadequate, especially if the threat increases dramatically.

The American Association of Port Authorities expressed concern about security for military mobilization. In written comments to the Commission, it recommended that the Departments of Defense, Transportation, and Justice support and participate in the ongoing efforts to review wartime vulnerability and peacetime security needs of U.S. ports. The Association asked that this be coordinated with all relevant federal (military and civilian), state, and local law enforcement and security-related agencies, including port authorities.

The impact of maintaining the status quo probably would not be evident until an actual military mobilization occurred, but potential problems include increased vulnerability to terrorist attack, a slowdown in the outload of military equipment, and ultimately a degradation in the country's national defense capability.

The Role of Technology in Seaports

The use of technology can be a critical building block in the effort by both the private and public sectors to reduce crime and increase security in U.S. seaports. The increased use of technology should be part of the response to each of the major issues identified by the Commission: the prevention and investigation of terrorism and crime; military mobilization; and border control of passengers, cargo, and crew. While it is important to recognize that using technology is only one means to an end and not the end objective itself, adding the right technology at U.S. seaports can:

- Increase the effectiveness, efficiency, and safety of port operations and the enforcement of applicable laws and regulations.
- Decrease vulnerabilities to criminal activities.
- Serve as a force multiplier for port operators and enforcement agencies.
- Enable new capabilities for port security and control.
- Facilitate quick responses for military mobilization, terrorist threats, and new requirements.

Technology can assist federal agencies, ports, and the private sector in the following areas:

Security equipment and technology is useful for establishing and controlling physical boundaries around and within the seaport. Examples of this type of technology/equipment are fencing and gates, access control systems, surveillance cameras, and communications equipment. Increased security technology at U.S. seaports can deter and defeat potential threats to seaport operations, minimize cargo theft and the illicit movement of materials into and out of the country, protect passengers and crews against criminal attacks, and protect vital national defense assets during military mobilizations.

Monitoring/surveillance equipment can be used to collect and record evidence of illegal actions and to record events occurring within the port. Examples are audio intercept, electronic surveillance, and tracking devices. Also included in this category are technologies appropriate for a first response to warnings of terrorist threats, hazardous incidents, and other special security concerns. Surveillance technology encompasses the broad set of electronic, audio, video, forensic, and other devices and systems used by criminal investigators to prevent crime, to enable the recovery of stolen goods and the seizure of contraband, and to bring criminals to justice. In this report, surveillance is cited as a key means of addressing the Commission's issues of preventing and detecting terrorism and crime, cargo control, and passenger and crew control at seaports.

Contraband detection technology is used to examine cargo, containers, conveyances, and persons for the presence of illegal or controlled materials entering or leaving the seaport. Examples are sensors to detect traces of explosives, drugs, or nuclear radiation; systems using gamma and X-ray imaging or neutron interrogation techniques to detect specific or anomalous concealed materials; and devices to detect concealed compartments.

Less than 10 years ago, the technology available to detect concealed materials in cargo or conveyances consisted primarily of small, low-powered X-ray units to examine baggage and small parcels, and hand-held devices such as fiber optic scopes, steel probes and needles, gamma backscatter units, and electric drills, which were generally limited to examining small sections of the suspect item. Using this equipment to thoroughly examine a truck and its cargo was time-consuming, labor-intensive, and frequently destructive.

Today, as a result of greatly increased congressional support and funding in the past decade for the development of new

drug detection technologies, new inspection systems now becoming available can examine entire trucks or containers in just minutes and provide a very high probability of detection of drugs, currency, explosives, and radioactive materials.

The technology categories are not necessarily exclusive. For example, closed-circuit television cameras around a seaport perimeter are part of security, but if a theft occurs they also can be used in the investigative activity that follows. Similarly, radiation detectors at a truck gate support both security and contraband detection.

A complete description of security, surveillance, and contraband detection technology is available in Appendix E of this report.

Technology and Equipment at Seaports

Federal inspection agencies, including Customs, the Food and Drug Administration, the Animal Plant and Health Inspection Service, the Food Safety Inspection Service, and the Fish and Wildlife Administration, have an interest in maintaining the integrity of cargo arriving from foreign countries. If cargo is stolen, not properly manifested, or improperly secured, it affects the ability of the federal agencies to carry out their functions of ensuring that cargo complies with U.S. laws and regulations.

Each year millions of shipments (many of them containerized) enter and exit the United States through the seaports. Federal agencies such as Customs, the Coast Guard, Immigration, and Agriculture that are charged with targeting and detecting contraband (e.g., drugs, illegal merchandise, organized alien smuggling, and stowaways), as well as weapons or explosives, in these shipments can examine only a small number of these targeted shipments through conventional means. Conventional means include surveillance, stripping containers and opening boxes, searching vessels, performing selective document checks, and patrolling areas where vessels dock in seaports. This is a labor-intensive process requiring many hours. Because appropriate technology for examining containers and shipments is limited at seaports, shipments may go unexamined.

Non-intrusive examination technology does exist that would allow federal inspectors to examine shipments quickly without opening containers. This technology is described in detail in Appendix E. During the seaport visits, the Commission found that the gamma ray system (at Port Everglades), a mobile truck X-ray system (in Miami), and weapon detection devices were being used to examine shipments entering or exiting the United States. The shipments were targeted because officials considered them high-risk for contraband, weapons, or explosives.

The identification and deployment of examination technology at many of the major ports along the southern land border, and at a limited number of seaports, has greatly enhanced the ability of Customs to examine high-risk shipments and containers entering the United States and to detect contraband and narcotics entering and exiting the country. The use of weapon detection devices at airports (by airline security personnel) and seaports (by the cruise line industry) has also resulted in the effective and efficient screening of passenger and baggage for weapons and explosive devices.

The Commission also found during its seaport visits that equipment such as cameras, carbon dioxide detectors, small boats, and vessel tracking devices that could assist law enforcement personnel in accomplishing their missions was available to field personnel in very few seaports. Immigration in Miami, for example, has a small boat to patrol the Miami River area, and Customs has, or is in the process of installing, cameras in the Ports of Jacksonville, Gulfport, Miami, and Port Everglades to assist in monitoring activities within the ports. The Coast Guard uses

vessel tracking systems in the Ports of New Orleans and Los Angeles to track vessels within the limits of the ports.

The identification and deployment of equipment that can assist law enforcement personnel in accomplishing their missions is critical. Devices such as cameras and vessel tracking devices that are useful in monitoring vessels and activities at piers, and carbon dioxide detectors and small boats that can be used to detect aliens and monitor "seaside activities" at seaports, can enable law enforcement personnel to work more effectively and efficiently.

Both the technology that is in use and the rudimentary forms of security vary from port to port. The majority of oil terminals and refineries that the Commission visited provide the benchmark for the use of technology and equipment. Most have more than adequate perimeter fencing (chain-link with barbed-wire top-guards in place). Lighting is designed to minimize shadows. Closed-circuit television is used to complement, not substitute for, manned security. Continuous vehicle patrols are made of the perimeter areas where possible, as well as in the interior. Berms are often in place along perimeter areas. Security vehicles have a radio link to each other and to a central command site. Employee parking is limited to a designated area. Firearms are prohibited for the most part.

The use of technology and equipment at other types of terminals, as well as at the ports themselves, is less substantial. Where perimeter fencing exists, it is in good repair, but there are ports and terminals where fencing is simply not in place. Commission members did not visit the ports or terminals at night, but it is clear from the placement of lighting that some facilities are not well lit, even though lighting for the most part is adequate. Closed-circuit television equipment is very limited, and many terminals do not have regular perimeter or internal vehicle patrols. Where a port has more than one entrance, there is often no means of communication between them. However, it should be realized that depending on the type of cargo at the port, the physical security in place may be sufficient. For example, most of the cargo on site at the Port of Detroit is steel for the automobile industry, which is not a highly desired target for theft because of its weight and bulk.

Although few seaports had X-ray technology, there were a few like Miami and Port Everglades that had basic non-intrusive detection technology. For the most part, seaport technology has lagged substantially behind that available in the nation's airports and on the Southwest border of the United States.

During its on-site surveys at the 12 seaports, the Commission found that the following technology (which was described in this chapter) was prevalent, or available for the use of law enforcement personnel: pallet/mobile X-ray systems, personal radiation detectors, contraband detection kits, covert surveillance equipment (including tagging and tracking devices), cameras, and sonar devices.

The Commission also found that the private sector has deployed the following technology at some of the12 seaports (or private terminals/facilities within seaports and the environs): vehicle tagging/tracking devices (for access control and accountability), closed circuit television cameras, trace detectors (for identifying the presence of drugs, explosives, or other contraband), infrared sensors, magnetometers, vessel tracking systems, and baggage/parcel X-ray systems.

Technology at the foreign ports visited (Felixstowe and Rotterdam) included large scale non-intrusive technology and closed circuit television cameras. The equipment deployed by both the government and the private sector in ports visited in the United States and overseas has proven beneficial in detecting both contraband and criminal activity at the seaports.

Even the most basic technology has shown results where it has been used. For example, in Miami, federal, state, and local law enforcement joined efforts to X-ray containers that were scheduled to be exported in an effort to identify stolen vehicles that were being illegally exported. Stolen cars are a major problem in South Florida, and law enforcement officials believed they were being smuggled in ocean containers. Using very low-resolution equipment that processed very rapidly, law enforcement officials were able to X-ray every container entering the yard to check for stolen vehicles. The process required only about 3 seconds, and cargo was not slowed down at the gates.

During the first month of the special operation, law enforcement officials were able to identify scores of stolen vehicles and return them to their owners. However, once the culprits were apprehended, the smuggling through the Port of Miami virtually stopped. Interestingly, the stolen car rate in Miami-Dade County declined substantially. The rate did increase, though, in Broward County, immediately north of the Miami seaport. Law enforcement officials were able to determine that the smugglers had shifted and were using Port Everglades to export stolen vehicles. The equipment that had been purchased by the state of Florida was then moved to another port.

Several of the agencies with work at the seaports could benefit from technology. Rather than each agency pursuing its own needs, it would be more cost-effective to develop shared technology at shared facilities, avoiding duplication of effort. Federal agencies could share facilities at seaports to share costs and also improve enforcement coordination and cargo inspection. The stakeholders at the seaports the Commission visited and in the MarineTransportation System report also recommended this course of action.

Responsibility for Improving Security at Seaports

During its reviews, the Commission found that the primary federal agencies having a primary interest in seaport security (Coast Guard, Customs, and Immigration) were not routinely performing security surveys and vulnerability assessments, nor were they participating in initiatives with the private sector to identify and address security-related deficiencies within seaports.

In the airport environment, the Federal Aviation Administration has dedicated staffs who work closely with airport authorities, carriers, vendors, and federal agencies at airports to identify and address security-related issues. Once the issues are identified, action plans can be developed and implemented to address the specific deficiencies or threats. Similarly, in the seaport environment, the Coast Guard, Customs, and Immigration and Naturalization Service should all have a strong interest in seeing that issues related to port security in seaports are identified and that these issues are addressed.

As discussed in Chapters 2 and 6, everyone involved at the seaport should have an interest in security. The private sector should be interested in preventing its cargo and facilities from attracting criminals. The port authority should be interested in preventing the port from being a haven for criminals. Law enforcement agencies at all levels should be interested in deterring crime, and entities that fund law enforcement should be interested in prevention, thereby reducing the need for expensive investigations and prosecutions.

As mentioned above, several federal agencies have a direct or indirect interest in security activities at the nation's seaports. What is needed is a mechanism to ensure that security interests in the seaports are carried out in a coordinated, cooperative manner. The overarching issue is who should take the lead.

According to Presidential Decision Directives (specifically PDD 63), it is the policy of the United States to ensure the continuity and viability of critical infrastructure, and to take all necessary measures to swiftly eliminate any significant vulnerabilities to both physical and cyber attacks on critical U.S. infrastructures. Because the targets of attacks would likely include both facilities in the economy and those in government, the elimination of potential vulnerability requires closely coordinated efforts of both the public and the private sectors. To the extent feasible, the federal government should seek to avoid outcomes that increase governmental regulation or expand government mandates to the private sector.

Applying this policy to seaports is a difficult task. Seaport terminals are a mix of government-owned and privately owned. The larger seaports are generally owned by the state or local government or a port authority that is part of some level of government. Many privately owned terminals may deal with only one or two commodities. Even ports that are publicly held may be operated, in whole or in part, by the private sector, so private sector cooperation is necessary.

Clearly, protecting seaports as described in the President's guidance on critical infrastructure will require a lead federal agency. The directive also designates the Secretary of Transportation as the lead for critical infrastructure that is transportation-related. The Coast Guard has a long-standing overall mission to foster seaport security, it has many specific missions related to this function, and it has experience in port security. The Coast Guard also has in place a Captain of the Port structure, which means that every port in the United States already has a designated Coast Guard officer with existing responsibilities. The Coast Guard clearly has the lead responsibility among the federal agencies for waterway security and safety issues. However, Coast Guard landside authority may be limited to waterfront facilities.

Customs has broader landside authorities for ports with international cargo. Its jurisdiction for security includes port authorities, carriers, brokers, truckers, railroads, foreign trade zones, and bonded warehouses. Customs jurisdiction extends to any place where international cargo has not cleared federal import or export requirements, even if it is 1,000 miles away from the port of entry.

The FBI is the lead agency for combating and responding to acts of terrorism. It has both investigatory and operational lead federal agency authorities when the issue involves terrorist incidents occurring within U.S. territory or in international waters. In addition, the FBI has Joint Terrorism Task Forces in major cities, and it actively manages terrorism programs in each of its 56 field offices and 400 resident agencies.

Port security is a broader issue than any one agency. The Coast Guard covers all seaports, but only on the water and at waterfront facilities. The Department of Defense has major security interests in 13 Strategic Seaports in times of military mobilization. The FBI has jurisdiction over numerous federal violations, including terrorism—this jurisdiction is not specific to the seaports. Customs has broad authorities for all passengers, cargo, and crew, and their movements until they clear Customs—but this jurisdiction covers only international seaports.

While everyone (federal, state, and local) is responsible for some aspect of seaport security, we believe the Coast Guard should be appointed the lead federal agency for coordinating seaport security. Further, we believe that national and local port security coordinating committees should be established that would include not only all the interested federal agencies but also other governmental and private sector interests.

One Size Doesn't Fit All

Throughout the Commission's review, it was evident that the threats faced by U.S. seaports varied for each seaport as a whole and for locations within the seaport. Because there are 361 seaports of many sizes and characteristics, it is reasonable to expect security requirements to vary from location to location. A rational scheme for the largest seaports like New York, Los Angeles, and Long Beach, which are dealing with large volumes of cargo, would be very different from a scheme appropriate to a port that has just a few vessels a month. Seaports with cruise ship passengers have special requirements. Requirements for security at seaports with major criminal activity such as New York, Miami, and Port Everglades will be different from the requirements at ports like Tacoma and Charleston that do not appear to have as large a crime threat. Within seaports, the security requirements for petroleum and other hazardous cargo will be different from those for iron ore or sawdust.

Another issue is response to incident-specific threats. It is not realistic to expect a security system at seaports that could accommodate a worst case scenario at all times, but a flexible system, involving a minimum level of security that can be raised during serious threats, is a reasonable expectation. For example, if the United States receives information that terrorists have planned a major assault on U.S. seaports and action is imminent, a system should be in place that could be augmented as needed to deal with that particular threat.

Governance and Delivery of Security Services in Seaports

In light of the recognition of seaport crime and security as a national security issue, the Marine Transportation System Task Force deferred to the Seaport Commission to undertake a comprehensive study of the nature and extent of the crime problem and state of security in U.S. seaports. The recommendations of the Task Force addressed areas for action that included facilitating collective action; developing coordinated interagency approaches; and evaluating existing programs or encouraging new programs that will produce the qualified, well-trained government and private sector personnel needed for implementing seaport security plans and operations. The Commission agrees that these are crucial issues and that deficiencies in these areas present significant problems to countering crime and improving security in U.S. seaports. During its work, the Commission found deficiencies in the state of security in seaports that led to the following effects:

- Enabled criminals to generally exploit vulnerabilities within the marine transportation system.
- Encumbered efforts against the types of organized criminal enterprises that target seaport commerce.
- Enabled internal conspiracies involving the acquisition of cargo transaction data and other forms of facilitation.
- Enabled criminals to operate fictitious or front firms for exploiting seaport commerce.
- Enabled criminals to operate extra-regional and transnational alliances for trading stolen goods and illicit services, and for facilitating other illegal transactions.
- Impaired sharing of federal, state, and local law enforcement intelligence and information with port authority security personnel.
- Focused attention on the limited presence of law enforcement and private sector countermeasures deployed in seaports, and the lack of integrated coordination between crime prevention and police efforts.

Blending Crime Prevention and Police Enforcement

The Commission observed that the most effective seaport security services consist of a blend of crime prevention and enforcement components, each of which have proactive and responsive aspects. Thus, quality of security in a seaport jurisdiction is the product of the combined effect of both crime preventive and police enforcement approaches.

The integration of crime prevention countermeasures and police enforcement operations, therefore, offers the best prospect for delivery of the most effective security services in seaport jurisdictions.

Crime prevention in seaports may include security surveys and vulnerability assessments, installation and monitoring of surveillance equipment, patrol and first-response to indications of detected crime, and communicating alerts for summoning a coordinated law enforcement community response. Crime preventive approaches do not require arrest authority and are typically carried out in U.S. seaports by non-police personnel, who may be employed by port authorities or private security firms. Large private sector firms operating within the port authority jurisdiction typically exercise crime prevention security practices in some form, either through their own staffs or contract personnel, although small independent tenants of seaports seldom employ such capabilities.

Conversely, enforcement action is primarily characteristic of seaport police departments empowered with the arrest authorities typically vested in state or local law enforcement agencies. Such enforcement activities involve the full range of operations characteristic of police agencies, including crime prevention patrol, developing and managing informants, coordination of multijurisdictional investigations, undercover operations and electronic surveillance, execution of search warrants, and arrest of criminals. Port security departments that lack law enforcement powers are limited in their capacity to coordinate with police agencies and are seldom included in the exchange of law enforcement intelligence used to counter organized criminal activity in seaports.

Observations of Current Practices

During its survey of U.S. seaports, the Commission found that port authorities were typically state or local governmental agencies that provided security services, if at all, through a variety of different organizational arrangements. The crime prevention approach was predominant and was carried out primarily through staffs of non-police personnel. In several seaports, most notably the Port of New York/New Jersey and the Port of Los Angeles, both crime prevention programs and law enforcement operations were delivered through port authority police departments. In those port authorities, security services were effected through comprehensive and coordinated crime prevention and police enforcement operations that were routinely integrated with other relevant federal, state, or local law enforcement operations (and on occasion with foreign police agencies), as well as with the security programs of private sector tenants.

Within other port authorities, less robust security services were provided through an arrangement consisting of an in-house security division staffed with non-police personnel, augmented by the operational presence of the local law enforcement agency of the jurisdiction in which the seaport is located. Within these port authorities the resources committed to the delivery of security services varied considerably. The following examples—Port Everglades and the Port of Miami—are seaports that do not have port authority police departments. They are instead attempting to combine an in-house security division conducting crime prevention with the law enforcement resources of the county police agency from the jurisdiction in which the seaport is located.

At Port Everglades, the port authority security staff seemed adequate in numbers compared with the size of the complex. The staff has received specialized training in seaport security and conducts crime preventive operations under the management of a public safety director who is guided by a written port security master plan. This security operation is augmented by a unit of the county's police agency consisting of officers and administrative staff totaling more than 60 personnel, the commander of which coordinates closely with the port authority public safety director. The county police personnel had not, however, undergone any specialized training in seaport policing, nor had they necessarily been selected for duty because of their relevant professional experience.

At the Port of Miami, the security staff seemed fewer in numbers compared with the size of the complex. They had received little in-house training, but operated under the guidance of a port security plan. The staff operations were augmented by a small cadre of the metropolitan police, the commander of which has direct supervisory control over the port authority security division. However, the port authority and metropolitan police are each independent departments of Miami-Dade County. It seems inevitable that separating the reporting lines of authority within a seaport jurisdiction would not provide the most effective arrangement in the long term for delivery of high quality security and police services.

The Policy Framework for Effective Seaport Security

The quality of seaport security is a matter of public interest, and the engagement of all levels of government is necessary to support seaport security requirements and minimize jurisdictional fragmentation of responsibilities. The Commission believes that in order to accomplish requisite objectives, a well-defined, coherent, and consistent policy framework for governing the planning and implementation of seaport security strategies and operations, at the national, state, and local levels, is of paramount importance to achieving successful results. Cohesive governance is also a key factor in successfully developing U.S. operating guidelines and minimum security standards, along with a strategy and process to enable their advancement on an international basis. Recognition of those advantages gives rise to the reasonable expectation that governmental port authorities would decide, at a minimum, to retain enforceable oversight of the security plans executed by private sector tenants within their port facilities.

Advancing further the concept of state and local government responsibility, it would again seem reasonable that the government jurisdiction in which a seaport is located would decide to take lead responsibility as the primary provider of police enforcement operations and oversight of crime prevention programs. Without a policy framework that facilitates unity of purpose, it seems unlikely the United States will develop integrated coordination of federal, state, and local security and law enforcement resources for achieving high quality crime prevention and police responsiveness to an organized criminal threat in seaports.

Professionalization of Private Security Providers

The Commission has received several suggestions about the private security guards frequently used at seaports. Many respondents stated that the employees did not have the training or expertise to do an adequate job. The view was frequently expressed that as long as the front line of security did not have the requisite skills, security would not be adequate.

During December 1999, the Commission traveled to the Netherlands to observe cargo control and port security practices and to learn more about that country's program for professionalizing and accrediting security personnel. In the Netherlands, no one may work as a security guard without a General Security Officer diploma issued by the national government. To obtain the diploma, all private security officers must be graduates of government-approved security courses and must pass national exams. In 1937, the Netherlands government, under authorization of the Militias and Private Security Organizations Act, established standards and performance levels in core competencies for security officers.

For the managerial and supervisory levels, training is provided in risk management, fire, social risks (labor disputes, police referrals, entry into property, etc.), burglary prevention, access control, fraud, embezzlement, internal corruption, sabotage, vandalism, industrial espionage, terrorism, and crisis management. This level of training is targeted at the company employee eligible for advancement. A collateral set of training classes is offered for those responsible for health and safety concerns. This training covers life-saving, fire prevention, first aid, wound bandaging, hazardous materials handling, and workplace safety.

The result of having a national standard has been the professionalization of the private security industry with nationally established job performance standards and a transportable credential (General Security Officer certificate) from the Dutch Government that provides employment opportunities and is a source of pride for the holder. Port security guards in the Netherlands are competent professionals and full partners with local and national law enforcement entities.

Findings

Finding 5.a. Presidential Decision Directives state that the federal government should play the lead role in bringing together the private sector interests in protecting critical infrastructure. Applicable PDDs do not call out seaports or responsibilities specifically.

Finding 5.b. The federal government has established formal structures for coordinating government efforts and developed national strategies to address drug trafficking, terrorism, and other domestic and international crime, military mobilization at seaports, and airport security. Seaport security per se, however, has not been adequately addressed. Stronger and more focused interagency and public/private sector efforts to enhance seaport security are needed to address the threats of crime and terrorism, and to enhance control of imports and exports, in order to meet national security and economic mobility requirements.

Finding 5.c. Although there are national efforts, many of them have not yet reached the level of individual seaports. Seaport authorities are often unaware of terrorism and crime threats and how security could lessen vulnerabilities.

Finding 5.d. Seaport security is a complex issue that involves federal, state, and local governments, port authorities, and hundreds of businesses; coordination related to seaport security measures is generally inadequate, in part because security-related meetings are not held in most seaports.

Finding 5.e. Federal, state, and local governments; port authorities; and private sector operators have not given adequate attention to seaport security issues.

Finding 5.f. Security measures and limits to access to seaports and terminals vary from port to port but are generally fair to poor. In a few cases, they are good.

Finding 5.g. No minimum security standards or guidelines exist for seaports and their facilities.

Finding 5.h. Responsibility for seaport security is fragmented.

Finding 5.i. Intelligence and information on seaport security matters is not consistently shared with all who need it.

Finding 5.j. There are few vulnerability or threat assessments of seaports and their facilities.

Finding 5.k. Current staffing allocations within federal agencies (such as the Coast Guard, Immigration, Customs, and Agriculture) do not permit them to dedicate resources to perform security surveys and vulnerability assessments, and to work with the trade to improve/enhance security within the seaports.

Finding 5.l. Procedures for restricting access to sensitive areas at terminals are inadequate.

Finding 5.m. At many seaports, the access of privately owned vehicles and commercial vehicles to vessels, cargo receipt and delivery operations, and passenger processing operations is not controlled.

Finding 5.n. At some seaports, local policy and/or agreements with the local labor force restrict the presence of firearms, but at most ports, the carrying of firearms onto the seaport is neither restricted nor controlled.

Finding 5.o. In some ports, there is mistrust and a lack of cooperation and communication between labor and federal law enforcement agencies.

Finding 5.p. Technology is available that can substantially improve the detection of criminal acts within seaports and contribute to overall security.

Finding 5.q. Security-enhancing technology is not available at most seaports.

Finding 5.r. Equipment (such as cameras, carbon dioxide detectors, small boats, and vessel tracking devices) that could assist law enforcement personnel in accomplishing their missions is not always available to field personnel.

Finding 5.s. Facilities (terminal operators, trucking companies, railroads, oil facilities, warehouses, etc.) surveyed did not meet all of the minimum standards established by the Commission for effective cargo security.

Finding 5.t. Seaports do not have separate and restricted areas where vessels, cargo, and passengers arriving from foreign locations are processed.

Finding 5.u. Areas in which federal inspection (Customs, Immigration, and Agriculture) takes place are not well-controlled, which poses a security risk to federal inspection personnel.

Finding 5.v. Passenger processing facilities for cruise ships do not provide the security needed for federal officials to undertake their inspections and related efforts associated with international travelers and crew members.

Finding 5.w. Cruise ships have worked cooperatively with federal officials to provide electronic passenger manifests, but officials still need detailed and accurate crew manifests.

Finding 5.x. The continuing increases in international passenger and crew arrivals have placed increasing strains on the current inspection processes of the Immigration and Naturalization Service. With these increases have also come increases in stowaways and alien smuggling.

Finding 5.y. The process of clearing and, where necessary, targeting cargo is complex, and highly dependent on robust Federal automated data systems and information provided by the importing and transportation communities in the private sector.

Finding 5.z. Vessel manifest information, import and export, is sometimes deficient for the purposes of import risk assessment

and export cargo control. Vessel manifest information is more easily utilized for drug enforcement and commercial compliance efforts if it is received in electronic data formats before the arrival of the vessel.

Finding 5.aa. The Customs in-bond system for the movement of foreign or restricted merchandise through the United States has been abused by violators, who have succeeded in denying revenue to the government, endangering American consumers, and compromising international trade agreements. Internal controls in the in-bond system would be improved if the level of information required for in-bond authorization were enhanced and received in an electronic format.

Finding 5.bb. Inadequacies in the cargo control processes used by federal inspection agencies provide opportunities for violators to exploit the system. Better information received in advance of shipment arrival via electronic data systems would promote improved cargo control processes.

Finding 5.cc. The federal agency automated systems are not easily accessible from waterfront cargo facilities or remote container examination stations. Lack of ready access impedes service level efficiencies, enforcement activities, and commercial compliance initiatives.

Finding 5.dd. The numbers of uniformed inspection personnel on the waterfront have been reduced over the past two decades, and the federal personnel involved in cargo processing usually do not coordinate their inspection efforts, nor do the various agencies share waterfront inspection facilities. Such discordant practices are inefficient for the government and burdensome for the trade and transportation communities. Shared federal inspection facilities, equipped with state-of-the-art high energy (X-ray or gamma ray) non-invasive inspection devices, and container devanning platforms located directly on the waterfront container terminals, would promote interagency efficiencies in cargo processing and provide economies for the importing and exporting public.

Finding 5.ee. Inadequate security, particularly existing cargo control measures, renders U.S. seaports vulnerable to those seeking to acquire or sell U.S. goods illegally.

Finding 5.ff. The shipper's export declaration—a key source of information used by law enforcement officials to identify illegal exports—is usually filed up to four days after the actual sailing of the vessel carrying the goods. This delayed filing privilege effectively removes any real controls from the administration of export regulations.

Finding 5.gg. Export enforcement efforts are hampered by inadequate electronic data systems and a compliance regime (fines and penalties) that may be inadequate to guarantee compliance with the export regulations.

Finding 5.hh. Differences appear to exist in the levels of resources devoted to export inspections and investigations as compared with import activity.

Finding 5.ii. Export control and compliance would be enhanced with better interagency coordination and improved educational outreach to the private sector exporting community.

Finding 5.jj. The fundamental weakness inherent in the in-bond system is the practice of allowing unexamined cargo to transit the United States. The raison d'être of in-bond, the deferral of duty and tax payments, would not be compromised if examination, for enforcement or compliance or safety purposes, were conducted before removal from the first port of arrival.

Finding 5.kk. The National Port Readiness Network/local Port Readiness Committee concept in the designated Strategic Seaports is fundamentally sound but in need of increased emphasis.

Finding 5.ll. Private security guards are a vital component of overall port security and cargo control. However, competencies in mission-critical tasks and service performance vary widely by security companies. The federal mission objectives of safe and secure ports are compromised if private security is unreliable.

Finding 5.mm. There is no existing system for testing the effectiveness of seaport security.

Finding 5.nn. The integrated coordination of crime prevention countermeasures and police enforcement operations led by the local jurisdictions offers the best prospect for delivery of the most effective security services in seaport jurisdictions.

Finding 5.oo. Separate lines of management between crime prevention security and police enforcement functions within a seaport authority jurisdiction encumber the delivery of high quality security and police services.

Finding 5.pp. The assertion of lead responsibility by the government jurisdiction in which a seaport is located, as the primary provider of police enforcement operations and oversight of crime prevention programs, will improve the integration, coordination, and effectiveness of federal, state, and local law enforcement resources with non-police seaport security staffs.

Finding 5.qq. Inadequate security hampers law enforcement efforts. Effective security measures are important tools for crime prevention and deterrence. Security countermeasures must be specifically designed to address internal conspiracies. In the majority of the seaports visited, there were no adequate security measures specifically designed to counter internal conspiracies, crewmembers drug smuggling, or alien smuggling.

Finding 5rr. Ports vary significantly in size and scope of operations throughout the United States. It is unrealistic to expect one standard security regime to be applicable to all ports.

Recommendations

Recommendation 8. Develop and propose new regulations to create a secure area (Federal Inspection Stations) in seaports where international passengers or passengers from foreign countries disembark. Customs, Immigration, and other relevant agencies should undertake this initiative on a joint basis.

Recommendation 9. Proceed with the Immigration and Naturalization Service Seaport Reengineering System Pilot Program for managing risk with respect to the admissibility of passengers and crew at the nation's seaports consistent with the President's 2001 budget request.

Recommendation 10. Establish, to the maximum extent possible, shared dockside inspection facilities (Federal Inspection Stations) at seaports for use by relevant agencies. Customs should take the lead with this initiative and coordinate it with implementation of the five-year technology plan (see Recommendation 15). Other relevant inspection agencies (e.g., Coast Guard, Food and Drug Administration, Agriculture) should conduct coordinated inspections and staff the Stations appropriately.

Recommendation 11. Undertake a comprehensive initiative to improve cargo import procedures and related efforts to target seaport crime. Customs, in consultation with other relevant federal agencies, should:

- Proceed with the development of the Automated Commercial Environment (ACE) and Automated Export System (AES) to ensure the adequacy of underlying Federal automated systems required to process commercial data/information.

- Propose revisions to its regulations to require that all ocean manifests be transmitted electronically to Customs sufficiently in advance of the arrival of the vessel to allow manifest information to be used effectively.
- Propose regulations, and, if necessary, legislation, requiring for all entries, including in-bond entries, the same level of information required for entries released into the commerce of the United States.
- Propose requiring that the above information be transmitted to Customs electronically before release of shipments for movement, including in-bond movement, from the port at which goods covered by the entry first arrive.
- Work closely with all other agencies having enforcement or regulatory responsibilities at the border to arrange for the above information to be distributed on a real-time basis to all agencies having an interest in the goods covered by a particular entry.

Recommendation 12. Strengthen the export enforcement programs, while preserving export facilitation, by proceeding as follows:

- The Department of Commerce should engage in rulemaking to require the electronic filing of export documentation for ocean shipping one day before a shipment's departure to facilitate targeting of illegal/illicit shipments and other criminal activity by law enforcement agencies. The proposed rule should provide for waiver authority for exigent circumstances. This information should be made available on a real-time basis to agencies with law enforcement responsibilities related to the seaports.
- The agencies with export enforcement responsibilities should update relevant regulatory authorities to increase fines and penalties (both administrative and civil) for export documentation violations, including provisions for enforcement personnel at all relevant federal agencies to issue on-the-spot fines for export documentation violations.
- All relevant agencies should strengthen government export document review programs aimed at enforcement of export control laws to increase export document review and identification of potential violations, and to increase export control-related investigations and enforcement activity, including legal support.
- Customs and the Office of Export Enforcement in the Department of Commerce should work jointly to improve effectiveness of existing resources by setting appropriate standards for seaports for export documentation compliance checks and by strengthening interagency cooperation.
- Commerce should develop a dedicated team at each Export Enforcement field office to work with Customs to target export control crimes and provide training to Customs on export control documentation as needed. Stakeholders, such as freight forwarders, should be targeted for compliance education and outreach by joint Customs and Commerce enforcement teams as needed.

Recommendation 13. Create, under the Marine Transportation System initiative, national-level security subcommittees of the Interagency Committee on the Marine Transportation System (made up of representatives from the federal government including Customs, Immigration and Naturalization Service, Maritime Administration, Coast Guard, Federal Bureau of Investigation, and others as appropriate), and the Marine Transportation System National Advisory Council (made up of representatives from the private sector including port authorities, ocean carriers, terminal operators, organized labor, truckers, warehouse propri-

etors, and railroads) to discuss, evaluate, and propose solutions related to seaport security and to address research and development, with emphasis on emerging technologies.

Recommendation 14. Develop, through the proposed national-level security subcommittee: (a) voluntary minimum security guidelines for U.S. seaports and their users that are linked to existing Coast Guard Captain of the Port controls of maritime trade; and (b) a model port concept, to include a list of risk-based best practices for use by terminal operators. The voluntary guidelines and the model port concept should take into account the differing risk levels and other security factors among ports and should be reviewed and updated at least every five years. To the extent that this approach does not promote significant and generally uniform security improvements at seaports within the next five years, alternative approaches should be considered, including making such guidelines mandatory. Consistent with Presidential Decision Directive 63, Transportation should be responsible for coordinating implementation, and the security guidelines should address, among other topics, the following:

- Uniform practices for physical security (fences, lighting, gates, etc.); for controlling the delivery, receipt, and movement of cargo, passengers, and crew; and for identifying high-risk individuals who seek access to sensitive areas within the seaport.
- A private sector credentialing process that limits access to sensitive seaport areas. This process should be administered by states, unions, port authorities, and/or port terminal operators. The national security committee should also assess the desirability and feasibility of utilizing criminal background checks to assist in determining access to restricted or sensitive areas at the seaports, including the advisability of port-specific approaches.
- Restricting the access of vehicles to seaports and facilities in seaports and requiring port authorities and the principal private sector businesses that use seaports to implement procedures that achieve appropriate control and accountability.
- Restricting the carrying of firearms in seaports.
- Developing a private security officer certification program to improve the professionalism of port security officers.

Recommendation 15. Develop, on a joint basis with all relevant federal agencies, a five-year crime and security technology deployment plan that addresses examination and investigative technology that can be deployed to seaports. Customs should take the lead in establishing a task force to develop a plan that considers utilizing existing mechanisms and programs, such as the Customs Border Integrity Project. This plan should address joint acquisition/use of equipment. Upon completion of the plan, appropriate funding should be sought through the regular budgetary process.

Recommendation 16. Strengthen, through the National Port Readiness Network, with Transportation and Defense as the lead agencies, the planning and coordination for military mobilization security at each Strategic Seaport. These efforts should include the following:

- Local Port Readiness Committees should actively participate in Department of Defense-sponsored combatant commander and Service mobilization exercises/cargo movements (in addition to their own biennial port readiness tabletop exercises) to ensure realism and efficient use of Department of Defense assets.

- The Department of Defense should assist the Coast Guard in establishing additional security guidelines for commercial facilities handling military cargo at the Strategic Seaports and for those seaports designated as Controlled Ports under Presidential Decision Directive 40.

Chapter 6: Coordination and Cooperation

One of the key objectives of the Interagency Commission was to assess the nature and effectiveness of the ongoing coordination among the federal, state, and local government agencies. As described in Chapter 2, a wide variety of entities exist in most seaports. The interests and missions of these entities are very frequently diverse and, in the case of law enforcement personnel, they often overlap. This chapter will look at how well the federal, state, and local government agencies and, to some extent, the private sector, coordinate and cooperate on matters concerning crime, terrorism, security, and federal inspection procedures.

Coordination and Cooperation Regarding Crime in Seaports

International trade at seaports makes them highly vulnerable to a wide range of criminal activity, and combating crime at seaports involves a wide variety of players. The distinction between federal or local responsibility for combating crime is generally based on what statute is being violated. If it is a federal statute, the federal government is responsible. If it is a state or local statute, the state or locality is responsible. If statutes of more than one jurisdiction are involved, any of those jurisdictions may prosecute.

For example, murder, assault, embezzlement, and theft at a seaport would generally be handled by the local jurisdictions unless it was related to organized crime or triggered some other federal statute. Drug trafficking that occurred at a seaport where only domestic cargo is involved could be pursued by the FBI or the Drug Enforcement Administration, or by state or local agencies. If federal agencies became involved, they generally would view the seaport not as a special entity but as just part of the city or jurisdiction in which the federal law enforcement officer operates.

Cargo theft is a crime of major concern to the private sector. It strikes directly at private entities' economic interests, and the Commission recorded dissatisfaction at the perceived lack of federal response to cargo crime at several seaports that we surveyed. Cargo theft is usually reported to the local law enforcement authorities and insurance companies. The FBI has long been active in responding to interstate cargo theft, working with local officials when possible. Customs and other federal inspection agencies also have a major interest in preventing cargo theft from the seaports. Combating crime on the waterways is primarily the Coast Guard's responsibility when federal statutes are involved. Coast Guard Captains of the Port commands are at all large ports and number several hundred people. The Environmental Protection Agency also has a major interest in environmental crimes on the waterways.

Exercise of state and local responsibility varies by jurisdiction. Many state and local governments have laws relating to ports and waterways in their jurisdiction and, in some cases, employ large law enforcement units for marine law enforcement. In many other ports, there is no local law enforcement presence in seaports or patrolling the waterways.

As explained in Appendix C, President Clinton approved two important strategies that relate to crime at seaports. The 1998 *International Crime Control Strategy* recognizes that international criminals engage in a wide range of illegal activities, including drug trafficking, terrorism, smuggling of aliens and contraband, fraud, extortion, money laundering, bribery, economic espionage, intellectual property theft, and counterfeiting. Most of these crimes occur at seaports. Because of the special border search authorities of agencies like Customs, Immigration, and the Coast Guard, seaports are a convenient and cost-effective location for combating these international crimes.

The 1999 *National Drug Control Strategy* established the framework for federal efforts directed toward drug trafficking. Drug trafficking has consistently been a major part of the role of Customs, the Coast Guard, and the Drug Enforcement Administration in and around the ports and on the water. Again, the special border search authority makes efforts at the seaport and on the high seas a productive and fruitful location to combat drug trafficking. In addition, interdicting drugs at their source or transit points is cost-effective.

The private sector has a responsibility to protect their property and facilities and to deter crime. Some take this responsibility more seriously than others. Some develop elaborate security systems; others do not choose to spend the money and instead rely on insurance to compensate them for the cost of crime and losses. Private sector entities have a wide variety of reasons for deciding what levels of security they will employ. However, once a crime is committed, it becomes the responsibility of the government at some level.

Although much of the information regarding crime is considered sensitive information and should not be released without a "need to know," law enforcement agencies, both interagency and intergovernmental, need to plan and coordinate their anti-crime efforts. We noted many successful examples of joint task forces or special operations that were interagency, intergovernmental, or both.

Coordination and Cooperation Among Law Enforcement Agencies

The Commission found that coordination and cooperation among federal, state, and local law enforcement agencies was good at the 12 seaports surveyed. The nature and extent of coordination efforts encompasses a wide variety of criminal activities, among a range of law enforcement agencies. The varied coordination efforts included drug smuggling, health and safety crimes, stolen vehicles and cargo theft, environmental crimes, and export control crimes. Some of the coordination efforts were solely among federal law enforcement agencies; other efforts included federal, state, and local law enforcement agencies.

A number of federal agencies and departments have memorandums of understanding that govern coordination and cooperation on law enforcement matters. For example, the Drug Enforcement Administration (DEA) and Customs coordinate and cooperate in drug smuggling investigations. Customs and Export Enforcement in the Department of Commerce coordinate and cooperate on certain export control investigations. The relevant law enforcement agencies in the Departments of Justice and Treasury also coordinate and cooperate on money laundering investigations.

Although much of the crime at seaports involves violations of federal laws relating to the importation and exportation of goods, most of the state and local law enforcement agencies support anti-smuggling efforts. In fact, some of the most successful law enforcement efforts were

accomplished at seaports where multi-agency task forces of state, local, and federal agencies addressed specific crime problems. Some of these task forces were funded through specific mechanisms, such as surcharges on insurance premiums to combat the export of stolen vehicles, or the Department of Justice Safe Streets Program to attack cargo theft. A number of task forces take advantage of the reimbursement of state and local overtime costs through federal law enforcement forfeiture funds, while others are encouraged by asset-sharing programs. Still other task forces were conducted under auspices of the High Intensity Drug Trafficking Areas or the Organized Crime Drug Enforcement Program.

The Commission found few stand-alone seaport task forces where agencies routinely met to discuss approaches to all types of crime at a given seaport. Rather, the task forces were focused on a particular crime, and the members consisted of the agencies with statutory authority in that crime. This kind of task force could be a formal standing task force, meaning that it met regularly and never disbanded, such as an environmental task force operating in Miami, Florida, or it could be informal and set up only for a specific duration, operation, or one-time initiative. By pooling resources and sharing intelligence, many agencies have found they can be more effective. Some federal agencies do not routinely join a task force because they lack the staff needed for full-time or even part-time participation, or because the major focus of their mission may not be seaport-related.

Coordination and cooperation among law enforcement agencies may be further improved by increased joint planning efforts and cross training. Increased participation in task forces and other effective interagency partnerships and initiatives between federal, state, and local law enforcement agencies may enhance coordination, cooperation, and responses to seaport crime.

The following are some examples, from the 12 seaports the Commission surveyed, of how law enforcement is responding to various aspects of seaport crime. These efforts are in addition to the task force efforts previously reported in Chapter 3. It should be noted, however, that many federal, state, and local agencies routinely work together in High Intensity Drug Trafficking Areas Task Forces, in Organized Crime Drug Enforcement Task Forces, and on a daily basis to address criminal activity relating to seaports.

Operation Winternight is a DEA and Customs partnership in which the DEA provides Customs with foreign drug intelligence about drug smuggling in containerized cargo. Customs obtains information on smuggling and smuggling organizations, which provides real-time investigative and interdiction information and leads. From fiscal years 1996 through 1998, 24 drug seizures totaling 11,162 pounds of cocaine were made at U.S. seaports based upon information provided by Operation Winternight.

A special project conducted by Customs, the Department of Transportation, and the Consumer Product Safety Commission targeted prohibited importation of cigarette lighters. The project targeted the smuggling of cigarette lighters without child-resistant safety devices into the United States. The project netted 30 seizures of nearly 4 million unapproved and unsafe cigarette lighters.

In January 1997, the Miami-Dade Auto Theft Task Force began electronic reporting at the Port of Miami. All vehicle identification numbers of vehicles presented for export were entered into a file that was sent to the National Insurance Crime Bureau (NICB) to run against the NICB database. If vehicles were stolen, if they had been exported before, if they had been salvaged, if the vehicle identification number did not conform, or if they were rentals, a message would be sent back to

the task force the following morning. The vehicles on this list would be checked before the exportation date.

The vehicles that were presented for export were checked against the National Insurance Crime Bureau database, but they only hit on the mirror image (stolen vehicles) of the National Crime Information Center database. In 1998, the FBI's Criminal Justice Information System created Project VINNY to allow checking also against silent hits and felonies. The data collected at the port would be sent to VINNY and the vehicle identification numbers would be run in the National Crime Information Center database to check for straight hits (stolen vehicles), silent hits, and felony messages. Each check would also leave a footprint for future reference. In addition, the Criminal Justice Information System would send the information to the NICB database for its checks. The NICB would send its messages back to the Criminal Justice Information System, and that System would create a list of vehicles to be checked and send it back to the task force. Thus, the information was more complete.

The FBI has implemented the Vehicle Theft Export database (VTED) to provide support to task forces targeting exported stolen U.S. motor vehicles. The primary goal of the VTED is to generate reports identifying criminal trends in modus operandi with shippers and consignees. The VTED captures the output results from VINNY via Law Enforcement Online. The FBI is attempting to identify patterns of exported stolen U.S. motor vehicles through date of export and the identity of the actual shippers. The port databases are being restructured to include the consignee field, which will support FBI efforts to identify patterns and organized groups or businesses creating and perpetuating the demand for exported stolen U.S. motor vehicles. As the VTED evolves, efforts will further be made to identify transshipment points for stolen U.S. motor vehicles located in foreign territories.

Recent Customs regulations implemented for the export of used vehicles appear to be sufficient to detect stolen vehicles, previously exported vehicles, salvaged vehicles, and vehicles with problem vehicle identification numbers. The regulations will be effective against criminals presenting vehicles for export, but they will not necessarily be effective against criminals concealing stolen vehicles inside containers for export.

However, the regulations, plus the Stolen Automobile Recovery System, an X-ray system, have proven very effective in combating the export of stolen vehicles at the Port of Miami. These X-ray systems can examine a container in an extremely short time, and hidden vehicles are easily detected. The Stolen Automobile Recovery System does not slow the incoming truck traffic. In a 90-day test period, more than 8,000 containers were examined with no false indications. The Port of Miami and Port Everglades both plan on purchasing these units.

The Environmental Protection Agency's Criminal Investigation Division, via a partnership with Customs, has addressed the importation of chlorofluorocarbons through Florida. The Criminal Investigation Division operates a standing environmental task force encompassing all state, local, and federal law enforcement agencies that have jurisdiction at the Port of Miami. It also has been very active in New York and has conducted a number of successful investigations in Puerto Rico.

The Environmental Protection Agency (EPA) has developed an initiative to familiarize Customs officials and brokers with the notification requirements and other compliance aspects of importing pesticides into the country. The effort has dramatically increased the number of import notifications received and has significantly strengthened the relationships between

the EPA, Customs, and the brokers and importers. The EPA hopes that it can gain routine access to Customs data it needs for evidence in its enforcement actions and for targeting companies that are not providing it with proper notification for imports of chemicals and pesticides.

The EPA has several civil enforcement initiatives encompassing seaports. One is the Voluntary Audit and Disclosure Export Notifications Initiative, which encourages companies to voluntarily disclose and correct Toxic Substance Control Act violations. Companies could volunteer by sending a notice of intent to audit their records for potential Toxic Substance Control Act violations. By September 1999, participating companies were to have audited and corrected any required notice violations. In return for companies' voluntary participation, the EPA issues a notice of noncompliance instead of a penalty action for these violations. As of September 9, 1999, 70 companies had registered to audit their facilities for violations.

In Seattle/Tacoma, EPA inspectors are accompanying Customs import specialists on joint inspections of selected chemical shipments. The EPA will conduct a compliance measures analysis and, as necessary, take follow-up enforcement actions against potential Toxic Substance Control Act violators.

Customs is currently cooperating with the EPA by providing records that will be used as evidence in an administrative case against a company for the sale and distribution of six aluminum phosphide fumigant products that it imported from China. Aluminum phosphide is inherently explosive and acutely toxic. All of the products the company has imported have been placed under bond and held by Customs. An import alert has also been issued to prevent any more of the products from entering into U.S. commerce.

The FBI's Newark Field office has established a Major Theft Task Force with the New York and New Jersey Port Authority Police Department. This task force, which handles major theft investigations such as cargo and vehicle theft in the Port of Newark and Port Elizabeth, has a number of significant port-related major theft cases pending.

New York and New Jersey have been cooperating on seaport crime-fighting for close to 50 years through the Waterfront Commission of New York Harbor. Congress established the Commission in 1953 with a mandate to investigate, deter, combat, and remedy criminal activity and influence in the Port of New York/New Jersey, and to ensure fair hiring and employment practices, so the port and the region can grow and prosper. Two commissioners, appointed by the governors of the two states, chair the commission. An executive director is responsible for day-to-day operations and oversees the six divisions: law; police; audit and control; executive; licensing and employment centers; and administration and management information systems. The commission has the authority to issue licenses and grant registrations and to conduct background investigations on certain employees of the port. The police division has full police powers in both states to investigate criminal activity relating to the port. Investigative accountants of the commission have authority to audit books and records of licensees for evidence of criminal activity and to ensure compliance with federal and state laws.

The commission conducts investigations on organized crime activity such as extortion, racketeering, gambling and loansharking, corruption, bribery, drug smuggling, cargo theft, and vehicle thefts. Many of these investigations are conducted jointly with appropriate state and federal agencies such as the FBI and Customs.

At the Port of New Orleans, Operation Government Against Theft on the River is a Customs initiative dedicated to the discovery and seizure of cargo stolen from the

port. Participants in this initiative include Customs, the Louisiana State Police, the New Orleans Harbor Police, and the New Orleans Police Department. Another Customs initiative in New Orleans, Operation Noose, is directed toward the detection and seizure of stolen conveyances and heavy machinery intended for export.

Agencies that may not have specific seaport enforcement operations or agency initiatives are responding to seaport crime as necessary. For example, the Immigration and Naturalization Service focuses the majority of its enforcement efforts at the land borders and airports rather than seaports, but through its investigations and anti-smuggling units it continues to develop intelligence to monitor alien smuggling. In August 1999, for instance, the Immigration and Naturalization Service received intelligence about alien stowaways on a vessel scheduled to arrive at Savannah, Georgia. The first inspection of the vessel for stowaways produced nothing, but additional intelligence led to the discovery of about 120 stowaways welded into the actual structure of the vessel. Without the information gathered by the Immigration and Naturalization Service, the stowaways would never have been detected. In the Los Angeles/Long Beach area, the Immigration and Naturalization Service has had a working group on alien smuggling and stowaway problems in effect for two years. These activities have proven instrumental in dealing with the current rash of alien smuggling interdictions on the West Coast.

Role of Port Officials in Identifying and Combating Crime

Some of the commercial port officials the Commission met with at the 12 seaports surveyed did not have a good understanding of the nature and extent of federal crimes associated with the importation and exportation of goods within their seaports. A number of officials either were unaware of the nature and extent of federal crime being committed or held the view that these crimes were not their problem. Many of these officials were primarily concerned with violent crime and property offenses being committed against seaport customers, employees, businesses, and property. Some officials seemed to use cargo theft as a benchmark for crime problems. They appeared to associate the level of crime in their seaports with their cargo theft problem. Some port officials stated that other types of crime, such as drug or alien smuggling or export crime, were the responsibility of the federal government and that if additional security or action was needed, the federal government was responsible for addressing those problems.

A contributing factor to these views may be that many of the law enforcement operations, initiatives, and investigations that agencies conduct are sensitive, and that laws, regulations, and agency policies limit the dissemination of information to port authorities. As a result, many port authorities do not know what types of federal crimes are being committed and the extent of those crimes. Without a complete understanding of the crime problems, it may be difficult for them to take crime issues seriously. This problem emphasizes the importance of collecting and reporting crime statistics by seaports. Crime reports could provide port authorities with the data, information, and assessments of the crime problems that they need to understand the effect of crime on their port operations.

Coordination and Cooperation Between Federal Agencies and Private Sector

Federal agencies have created several cooperative programs with the private sector to encourage joint efforts to combat crime at seaports. In many cases, maritime com-

panies involved in trade logistics have significant information and can readily identify suspicious importers or shipments. Through industry partnership programs, federal agencies enlist the industry's support in law enforcement initiatives. The agencies provide incentives to companies to establish practices that will prevent violations and reduce industry's vulnerability to criminal activities, and to report violations to law enforcement officials. These reports can result in the seizure of contraband and arrests and convictions of violators.

The Department of Commerce's Bureau of Export Administration initiated the Business Executives' Enforcement Team program. The program is part of Commerce's effort to prevent violations by educating and expanding contacts with U.S. business. The program, a series of half-day forums around the United States, allows corporate officials to learn about their responsibilities under U.S. export control laws, and to pose questions to senior export enforcement officials. The Business Executives' Enforcement Team participants explore ways for businesses and enforcement personnel to work together to prevent violations and identify projects of concern for proliferation reasons.

Customs has three major industry partnership programs: the Carrier Initiative Program, the Business Anti-Smuggling Coalition, and the Americas Counter Smuggling Initiative. Under the Carrier Initiative Program, Customs provides incentives, such as penalty offsets, to carriers to enhance their security practices and training to prevent carriers' conveyances from being used to import drugs into the country. Under the Business Anti-Smuggling Coalition, corporate participants (importers and exporters) and port authorities set self-imposed standards to deter narcotics smuggling and work with Customs to implement and share best practices. Under the Americas Counter Smuggling Initiative, Customs has expanded anti-narcotics security programs with industry and governments throughout Central and South America. These programs have also proven to be successful enforcement tools for Customs. From fiscal years 1996 through 1998, participants in these programs provided information to Customs that resulted in 175 seizures totaling 39,326 pounds of narcotics and assisted in 287 foreign interceptions totaling 73,854 pounds of narcotics destined for the United States.

The Immigration and Naturalization Service has a Carrier Affairs Office that manages and designs programs to educate carriers in the screening of passengers at ports of embarkation and in the examination of travel documents, including instruction on detecting fraudulent documents. These efforts attempt to decrease the incidents of aliens arriving in the United States without proper documents in violation of immigration laws. In addition, these training efforts assist carriers in reducing administrative fines imposed against them for boarding improperly documented passengers.

The Drug Enforcement Administration's Chemical Diversion Group provides assistance to the regulated private sector which produce legitimate products used by traffickers to manufacture illegal drugs. This involves working with associations in development of enforcement policies and regulations, sponsoring conferences and national and working committees, conducting annual seminars on the import/export application process, providing manual and customer service pamphlets, establishing industry points of contact with the Drug Enforcement Administration, and maintaining information on the Drug Enforcement Administration's Internet home page.

The Maritime Administration's Port and Cargo Security Program aims to reduce criminal exploitation of commercial maritime cargo, particularly drug smuggling, cargo theft, and related forms of transnational cargo crime in the Western Hemisphere. The Maritime Administration engages in cooperative efforts with govern-

ment and private sectors to develop seaport security improvements in the Inter-American region. It collaborates with multinational entities such as the Organization of American States, the American Association of Port Authorities, and the International Association of Airport and Seaport Police. In 1998, the Maritime Administrator addressed a summit of Western Hemisphere transport ministers and proposed the cooperative development of a strategic approach for improving the security of the Inter-American maritime trade corridors and reducing cargo crime, and was incorporated into the ministerial declaration. This directly influenced subsequent port security developments within the Organization of American States, with particular bearing on private sector development. Since 1995, the Maritime Administration has published the *Maritime Security Report,* an open source intelligence product that is disseminated widely to government and the private sector. In collaboration with the Organization of American States, the Maritime Administration also organizes and manages the Inter-American Port Security Training Program.

Coast Guard initiatives include Prevention Through People to exchange information between industry and the Coast Guard on maritime matters; Multi-Agency Strike Force Operations to stop illegal incidents in port areas; and Port State Control to facilitate foreign vessel inspections.

Partnership programs have been very successful and are a force multiplier for federal agencies. They should be continued, and expanded where appropriate. These issues are addressed more fully in Chapter 3.

Cooperation and Coordination Concerning Terrorism

On terrorism issues, the federal government has the clear lead in coordinating the nation's ongoing response. Clear guidance has been issued to the Executive Branch through Presidential Decision Directives (PDDs), which assign roles and responsibilities to appropriate federal agencies and set forth policy and procedures.

Many officials with whom Commission members spoke stated that law enforcement coordination and counterterrorism training at their seaports are satisfactory. Officials at other ports are not as confident in the level of coordination and training. Overall, there appears to be a need for an overall assessment of the training needs for seaport personnel to raise their awareness of terrorism issues.

As noted in Chapter 4, the various threat warning and response systems appear to be satisfactory and operating as intended.

Coordination and Cooperation of Security in Seaports

As mentioned in Chapter 2, seaport security could be considered to be under the purview of the ports and the entities who use the ports (carriers, terminal owners, warehouse operators, etc.). Some ports take this responsibility more seriously than others. Although security requirements could be directed by the states, they generally have not been.

The Secretary of Transportation, under Presidential Decision Directive 63, has responsibility for leading efforts to protect critical infrastructure in the transportation sector, which includes seaports.

The federal government also plays a role through the National Port Security Committee created in 1950 under the Magnuson Act. The Committee is under the aegis of the National Security Council and chaired by the Commandant of the Coast Guard. The committee deals with specific incidents such as embargoes and monitoring the entry of vessels that bear the flag of, or are under the effective control of, certain states that have been ident-

ified as threats to national security while operating in the territorial seas of the United States. Executive Order 10173 further directs all agencies and authorities of the United States government and all state and local authorities to support, conform to, and assist in the enforcement of this program.

The Coast Guard has the lead responsibility among the federal agencies for waterway security and safety issues. Its landside authority, however, may be limited to waterfront facilities. The Coast Guard's responsibility for port security, and for fulfilling other missions related to this function, is of long standing. Through the Coast Guard's Captains of the Port structure, every port in the United States already has a designated Coast Guard officer with existing responsibilities.

The Captain of the Port participates in Harbor Safety Committees, many of which were established by port. These committees generally include representatives from all the private sector interests involved in port activities. A national counterpart has just been created via the Interagency Committee on Marine Transportation System and the Marine Transportation Systems National Advisory Committee.

The security of international passengers and cargo is the concern of the Coast Guard and Customs. Customs has broad landside authorities for ports with international cargo. Its jurisdiction for security includes port authorities, carriers, brokers, truckers, railroads, foreign trade zones, and bonded warehouses. Customs jurisdiction is anywhere there is international cargo that has not cleared federal import or export requirements, even if it is 1,000 miles away from the port of entry. Customs has established voluntary security agreements with thousands of carriers, brokers, and freight forwarders and businesses in the United States and in high-risk countries as part of its antidrug efforts. Customs also has a pilot program to install security equipment in cooperation with port authorities, the private sector, and other federal agencies.

Enhanced security measures also serve to prevent crime, and for that reason security should be of interest to all seaport stakeholders. For example, law enforcement officials at all levels could view crime prevention as a way to reduce needs for additional resources. The private sector also has a major interest in reducing losses due to theft; a decrease in crime should make the private sector's operations more profitable.

Unlike some of the other areas covered in this report, security responsibilities are not clearly laid out. It is not clear who should do what. In some seaports, there may be an active interest in security and in others there may not be much. Most often, security programs are downplayed because of the perceived costs. Neither the federal government nor the state governments have taken the lead in this area. As described in Chapter 5, seaports handle day-to-day security in a variety of ways. The first responders for nonfederal crimes are generally local law enforcement. Some seaports have sworn law enforcement officers on-site, but most do not. In all ports and terminals, private security firms provide some form of security.

To a certain extent, the quality of coordination and cooperation between law enforcement agencies regarding security-related issues depends directly on two factors: the quality of training that officers receive and the clarity of definition of their roles. The 12 seaports that we surveyed had various types of law enforcement oversight, and the quality of training and the interrelationship among the various enforcement and security groups differed. At one extreme were ports such as New Orleans, Los Angeles, and New York/New Jersey, which had one police agency that was responsible for most of the policing at the port. The police officers were academy-trained, carried firearms,

and had general arrest authority. At the other extreme was a port such as San Juan, where an unarmed port security force with no general arrest authority was responsible for security.

Whether or not a particular port had a well-trained police force in place, all 12 of the seaports surveyed had multiple security agencies doing the policing. Container facilities, oil terminals, and passenger terminals often had private security in place. In Port Everglades, for example, port authority security staff, local law enforcement officers, contract security, and federal agencies all had some responsibility for security within the port, and in its terminals and facilities.

While a "layered" system for ensuring security at seaports is viable, what we found more often than not was that the policing and security functions were fragmented. Often it was unclear who was responsible for enforcement tasks. In most of the ports we found a lack of coordination among the various police and security personnel and a lack of common standards for ensuring security. The lack of common standards creates gaps that criminal elements can and will exploit. It also creates problems for stakeholders who are not sure whom to contact and who on occasion are left with the feeling that nothing is done when a complaint is filed.

The issue of fragmentation is only part of the problem inherent in a multiple law enforcement jurisdiction. The other part is the disparity in substantive knowledge, training, and capability in port security and law enforcement matters between the local police (including port police) and contract security personnel. Complicating matters is the fact that security personnel are often structured differently in each seaport. For example, in Los Angeles the port police are sworn law enforcement officers with full police powers and a dedicated waterside harbor patrol. Next door, in Long Beach, the Harbor Department's Security Division consists of non-sworn officers with no police powers and no dedicated harbor patrol capability. In the Port of Charleston, moderately trained state employees (port service officers) staff all entrances to the port's five central terminals. Relatively untrained contract security personnel guard San Juan and Long Beach's widely dispersed and numerous individual terminals. Several ports where a sworn police force is in place do have periodic meetings with stakeholders to discuss their concerns about security and to share intelligence information with them. At the Port of New York/New Jersey, police officers are assigned on a permanent basis to maintain contact and periodically conduct on-site visits to the tenants in the officer's area of responsibility. In addition, monthly meetings are held with tenants to hear their concerns, offer suggestions for improving their levels of security, and share intelligence. This community policing effort has been considered beneficial by the participants.

During the on-site surveys at Miami, Port Everglades, Los Angeles, Long Beach, and San Juan, we found an apparent mistrust of, and lack of cooperation between, labor and law enforcement agencies. In Miami there was a sense that labor felt that it was being wrongfully singled out for investigations into criminal activity. Federal, state, and local law enforcement agencies appeared to cooperate to a greater degree in Gulfport, Charleston, and Tacoma. In Tacoma, local law enforcement officials told the Commission the local union was helpful in combating crime. The most serious problem at the ports we surveyed is the failure of federal law enforcement agencies to cooperate with each other in regard to security matters and to share intelligence information. This is especially necessary where federal law enforcement is stretched extremely thin. The lack of cooperation appears to result not from a concerted effort on the part of the federal agencies to "go it alone," but simply from a lack of centralized organizational control in shar-

ing intelligence. Various representatives at the federal agency focus groups we held at all the seaports told us repeatedly that their agency worked very well with other agencies. The problem, however, is that these relationships tended to be reactive. A number of seaports that we surveyed do have joint federal agency meetings, but the meetings tend to be occasional, and it is not clear to the agencies who should take the lead in establishing the meetings and setting the agendas. Thus, once a crime has been detected, the agencies may work well together, but they rarely work together in planning or taking measures to prevent crime or other problems.

The on-site seaport surveys revealed that regular "security-related" local meetings were not being held in seaports between law enforcement organizations (federal, state, and local), the trade, and port authorities, with the exception of those relatively few Strategic Seaports (ports that support military mobilization) where port readiness committees are active. The meetings could provide the participants (government and private sector) with the opportunity to exchange intelligence information, discuss operational issues, and carry out action plans designed to enhance security in seaports and address deficient security practices within seaports. New Orleans is one port that used to have regularly scheduled meetings of principals to discuss security-related issues, but over time it has discontinued the meetings.

The *Marine Transportation System Report* recommended that a National Advisory Council be established to work with the large numbers of public/private sector interests in the maritime network. Coordination of the complex network of relationships and interests on security is critically important. A separate Security Subcommittee should be established as part of the Marine Transportation System to ensure that the recommendations in this report are carried out.

Coordination and Cooperation Among Federal Inspection Agencies

The clearance of international cargo is solely a federal government function. It involves 60 agencies and the enforcement of 600 laws and more than 500 trade agreements. Customs conducts inspection and review functions for most of the agencies, but the following agencies are often on-site or located near the seaports: the Food and Drug Administration, the Animal and Plant Health Inspection Service, the Food Safety Inspection Service, the Fish and Wildlife Service, and the Bureau of Alcohol, Tobacco, and Firearms. The Coast Guard, also located in or near every seaport, conducts its own inspections, particularly those dealing with hazardous materials.

Customs serves as the unofficial lead for the clearance of international cargo. It maintains the nationwide database for international cargo that is used by all agencies in the federal government. Although Customs has a five-year plan and an annual plan, the other federal agencies involved in international cargo clearance are not officially part of the plan. The agencies meet in headquarters and the field when issues arise, but there is no formal coordinating mechanism at either the national or the local level. There should be.

Despite the vast number of agencies involved in this border inspection and control function, there is no formal structure for planning and organizing the process. Each agency conducts its planning separately. They may consult one another, but there is no joint plan or process. With the complexity of the process and the large number of federal agencies involved, coordination is a necessity at both the national and local levels.

The co-locating of federal inspectors, with their electronic equipment, in Federal Inspection Station facilities at the docks where the cargo arrives would improve

cooperation, avoid duplication of effort, reduce costs in the long term, and support coordinated enforcement activities and promote customer service. The creation of the Federal Inspection Station is a necessary first step, and a very tangible step, in the right direction.

Assisting with the mission of interagency coordination and support is the Customs automated commercial system. The Customs automated system is a critical link to all the inspection agencies. Customs has placed criteria in its cargo release system for at least 12 other federal agencies, and it provides online access, data extracts, or other interfaces as reported below for a variety of federal agencies. Some agencies have access to one or more automated Customs systems; some, such as the Food and Drug Administration, have their own automated systems that interface with Customs; and others, such as Agriculture's Food Safety Inspection Service, do not use the Customs system at all. Many other agencies could improve their monitoring of international trade with real-time use of this system.

The Animal and Plant Health Inspection Service (APHIS) of Agriculture has access to the automated manifest but not the automated entry system, which has more detailed information on the merchandise and the country of origin. Most of the APHIS offices reviewed still use the paper manifest to target merchandise for inspection because of the lack of adequate descriptions and difficulty using the manifest data. The Fish and Wildlife Service receives data only from the entry system of Customs. The Food and Drug Administration developed its own system to pull in Customs entry data to automate its processing, targeting, and tracking activities. The Environmental Protection Administration is considering broadening data-sharing and coordination with the Customs Service. We believe it is in the interest of all federal inspection agencies to consider greater interagency exchange of data and sharing of information.

Many of the memorandums of understanding between Customs and other federal inspection agencies on the sharing of trade information are outdated and do not reflect the current information needs of each party. Although each inspection agency complained about the accuracy and completeness of the data in the Customs systems, an underlying issue appears to be that some agencies do not access or use the data that are already being collected. In fact, because many federal inspection agency employees do not have background clearances or sufficient procedures to safeguard trade information, Customs is prohibited from giving them complete access to the information it collects.

If the Customs automated systems are to remain the central trade-data collection system for all other federal agencies, Customs needs to enfranchise the other federal agencies in the developmental dialogue about new systems. An interagency group should be convened to develop long- and short-range plans to meet trade information needs. This group should focus on both improving the existing systems and developing criteria for the next-generation system to ensure that it supports each agency's regulatory role and facilitates information-sharing and user-friendly access for all participants. If the Customs automated systems are to remain the central processor and repository of trade data, the Customs Service should chair this committee.

The federal government is funding the improvement, deployment, and development of automated trade data systems for the commercial and enforcement needs of the federal agencies and their private sector partners in the arena of international trade. The federal agencies and the trade sector are dependent on the reliability and utility of these systems, and unless improvements are made to existing federal systems, dis-

ruptions in the import or export of cargo may occur. As previously noted, technology upgrades should be coordinated among all relevant federal inspection agencies to ensure that every agency's needs are being addressed and to promote efficiencies in the design and development of new multi-agency cargo control, entry systems, and enforcement systems.

Border control of international passengers and crewmembers is a federal responsibility. Immigration, Customs, and Agriculture must check all persons arriving from other countries, including crew of vessels as well as passengers aboard cruise ships, to ensure that they meet requirements to enter the United States. Immigration also must address alien smuggling at seaports. This is solely a federal function, but cooperation from the state and local law enforcement agencies and the private sector can be helpful. A prime finding of this Commission is the need for coordination and cooperation among the various federal inspection agencies that share responsibilities and interest in waterborne cargo (import and export). In an era of diminished resources, the creation of shared Federal Inspection Stations, equipped with adequate facilities for the examination of container load shipments, supported with state-of-the-art high energy X-ray devices and located directly on the waterfront (container terminal) properties is the right course of action if this country is to reestablish meaningful control over its seaport gateways.

Findings and Recommendation

Finding 6.a. Coordination and cooperation among federal, state, and local law enforcement agencies is good. The nature and extent of coordination efforts encompasses a wide variety of criminal activities, among a range of law enforcement agencies. Coordination efforts include drug smuggling, health and safety crimes, stolen vehicles and cargo theft, environmental crimes, and export control crimes.

Finding 6.b. Some of the most successful law enforcement efforts are accomplished at seaports where multi-agency task forces of state, local, and federal agencies addressed specific crime problems. However, some federal agencies do not routinely join a task force because they lack the staff needed for full-time or even part-time participation, or because the major focus of their mission may not be seaport-related.

Finding 6.c. Some commercial port officials do not have a good understanding of the nature and extent of federal crimes associated with the importation and exportation of goods and contraband within their seaports. Some port officials are primarily concerned with violent and property crimes and consider federal crimes such as alien smuggling or export crime to be the responsibility of the federal government.

Finding 6.d. Industry partnership programs between federal agencies and the private sector are notable and are a force multiplier for federal agencies. These programs have not only enhanced the security practices and training of the private sector, but they have proven to be successful enforcement tools in U.S. drug interdiction efforts.

Finding 6.e. The threat warning systems (the National Threat Warning System, the Awareness of National Security Issues and Response System, and the National Law Enforcement Telecommunications System) appear to be satisfactory and operating as intended.

Finding 6.f. Policing and security functions are fragmented at many seaports, and there is a lack of coordination among the various law enforcement and security personnel.

Finding 6.g. There is a disparity in substantive knowledge, training, and capabili-

ty in port security and law enforcement matters between the local police (including port police) and contract security personnel at many ports.

Finding 6.h. At some seaports there is an apparent mistrust of, and lack of cooperation between, labor and law enforcement agencies.

Finding 6.i. Regular "security-related" local meetings are not being held in seaports between law enforcement organizations (federal, state, and local), the trade, and port authorities, with the exception of those relatively few Strategic Seaports (i.e., ports that support military mobilization) where Port Readiness Committees are active.

Finding 6.j. Many of the memorandums of understanding between Customs and other federal inspection agencies on the sharing of trade information are outdated and do not reflect the current information needs of each party.

Finding 6.k. Seaport security is a complex issue that involves federal, state, and local governments, port authorities, and hundreds of businesses; coordination related to seaport security measures is generally inadequate, in part because security-related meetings are not held in most seaports.

Recommendation 17. Establish local Port Security Committees—or possibly a subcommittee of an existing Harbor Safety Committee or Port Readiness Committee—at seaports, including representatives from the port authority, federal, state, and local governments, and the private sector (including organized labor), to discuss and develop solutions for port-specific security issues. The responsible Coast Guard Captain of the Port should chair the local Port Security Committee.

Chapter 7: Intelligence and Information Management

Chapters 2 through 6 discussed the variety of government agencies and private sector entities involved in seaport security operations and their needs for intelligence and information to conduct their mission or business effectively. This chapter deals with that intelligence and information—which agencies are involved in gathering and providing it, what kinds of information are available, and what processes are used for disseminating intelligence on crime, terrorism, and port activities to those who need it.

The term "intelligence" is used here in a general sense, to describe the gathering of information by law enforcement agencies in support of broad investigative or general law enforcement initiatives, as well as the gathering and use of national-level intelligence by agencies of the intelligence community. Interviews with law enforcement agency personnel and maritime industry focus groups revealed concerns that information needed for seaport security was lacking in three principal areas, which will be the focus of this chapter:

- Availability to law enforcement agencies of relevant, actionable intelligence on seaport crime.
- Awareness of terrorist threats and availability of threat information to the private sector as well as federal, state, and local enforcement personnel.
- Integrated information on the movement of vessels, people, and cargo within seaports and ready availability of that information to government agencies and private sector security organizations.

The Role of Intelligence in Combating Crime

Intelligence is the product resulting from the collection, processing, integration, analysis and interpretation of available information. Collecting, analyzing, and disseminating intelligence is central to striking international crime at its source. Intelligence can pay substantial dividends in identifying trends in international criminal activities and in tracking the structure, networks, methods of operation, and vulnerabilities of international criminal organizations. Mechanisms must be in place to ensure that intelligence efforts are directed toward meeting the highest-priority needs of policymakers and federal law enforcement agencies. The intelligence community should enhance its efforts to provide detailed and timely information to U.S. law enforcement agencies to help them prevent international crime and dismantle criminal organizations. According to the President's *International Crime Control Strategy* (May 1998), international crime threatens vital U.S. interests in three broad categories: threats to Americans and their communities, threats to American businesses and financial institutions, and threats to global security and stability.

- International terrorism and drug trafficking most directly threaten American lives and property.
- Illegal immigration, trafficking of women and children, and environmental crimes may pose direct threats to safety, health, stability, values, and other interests of American communities.

- The illicit transfer or trafficking of products across international borders may undermine U.S. national security objectives. The tremendous volume of international traffic and trade provides international criminals tremendous opportunity to smuggle illegal aliens, drugs, and other contraband into the United States.
- Economic trade crimes such as the smuggling of contraband products, the violation of intellectual property rights through product piracy and counterfeiting, industrial theft and economic espionage, and foreign corrupt business practices may rob U.S. companies of substantial commercial revenues and may affect their competitiveness on world markets.

Many of these threats have a maritime component. Customs data show that in 1999 more than 200,000 merchant and passenger ships docked at U.S. seaports. They carried nearly 5 million shipping containers and 400 million tons of cargo into the United States. Customs physically inspects less than 2 percent of the goods transiting U.S. borders daily. *Threats and Challenges to the Maritime Security 2020,* published by the Office of Naval Intelligence and the Coast Guard Intelligence Coordination Center, states that "legal maritime trade, driven by global economic growth and flourishing international trade, will triple by 2020. The most explosive growth will be in the container shipping industry. The trend will be toward larger ships carrying more containers." Given these trends and the existing level of resources, it is likely that even less than 2 percent of arriving cargo will be inspected in the future.

Criminals have expanded the scope and range of their activities and have become more sophisticated in the conduct of their operations. Criminal organizations take advantage of growing global maritime trade to move products more efficiently. Many criminal organizations have extensive worldwide networks and infrastructures, including front companies, quasi-legitimate businesses, and investments in legitimate firms to support criminal operations.

Targeting Containerized Shipments

Intelligence is key to interdiction. In particular, it is essential to the aspect of maritime surveillance that attempts to identify a particular container being used to smuggle illegal drugs or other contraband. Intelligence for tipping off and directing interdiction operations is the only effective means to segregate most maritime smuggling targets from normal commerce. Without predictive intelligence, the detection and monitoring of ships is impossible, given the thousands of vessels found daily in the sea lanes. Intelligence collection and analysis must begin, for targeting purposes, before the shipment reaches its destination. To provide this focused targeting information at U.S. seaports, informants need to be cultivated in foreign countries who provide information on companies, individuals, and organizations involved in illicit trade.

Investigations of the use of freight containers for smuggling depend heavily on explicit intelligence provided by informants. As maritime container traffic volumes increase, random inspections become statistically less likely to detect concealed shipments. Review of shipping documentation by customs inspectors, although an increasingly effective tool, is also somewhat limited by the volume of container traffic. Labor-intensive searches of containers based on random selection are less productive than inspections prompted by explicit intelligence. Predictive, operational intelligence that provides explicit information usable at the tactical level can increase the probability that threats can be identified before arrival in U.S. ports, and that container inspections will result in contraband seizures and arrests. Smugglers will

likely continue to convert larger percentages of their illicit cargoes to commercial maritime freight containers. Development of intelligence sources, particularly human agents, that can provide information on specific shipments en route should improve interdiction results.

Information Exchange with the Private Sector

Government efforts to combat cargo crime will be enhanced by the increased awareness resulting from information exchange programs with the private sector. Information exchange is crucial to enlarging port and cargo security programs into cooperative alliances that can form an investigative bridge throughout maritime trade corridors.

Key coordinating processes that can result from information exchange include the following:

- The private sector's role in supporting government's requirements for actionable intelligence on cargo crime activities.
- The reciprocal role of government in providing industry with intelligence with which to implement effective countermeasures against cargo crimes.
- Joint training of seaport police and private sector security personnel.

Information provided by the maritime industry has proven indispensable to law enforcement in effecting multinational interdiction of alien smuggling, drug smuggling, and other cargo crimes at their source or in transit countries. Even if developed late in the shipping cycle, this source of intelligence continues to be instrumental in successful government interdiction of cargo crimes. In recent years, information derived from the Customs Service's private sector carrier initiatives has resulted in more drug seizures than has intelligence developed by federal agencies. Information exchange provides a basis for understanding the scope and magnitude of international crime. This approach can offer the government a mechanism for integrating the maritime industry into the process of preparing a comprehensive assessment of the international cargo crime problem. Inclusion of the private sector would add an indispensable dimension to the cooperative efforts of all U.S. law enforcement, diplomatic, and intelligence agencies.

Intelligence Support for Law Enforcement

Federal, state, and local law enforcement agencies interviewed indicated that intelligence collection and dissemination regarding criminal activity, particularly as it relates to foreign intelligence collection, needs to be improved. A common complaint was the lack of actionable international intelligence in the commercial environment. With current staffing and resource allocations, limited contraband detection technology, and the tremendous growth in trade, agencies need to have significantly more actionable intelligence to be effective.

Information-sharing and intelligence-gathering among federal, state, and local agencies at the ports is spotty and sporadic. A significant amount of foreign criminal intelligence is collected in the areas of drug trafficking, organized crime, money laundering, alien smuggling, and other criminal activities. However, specific, actionable intelligence or information relating to the importation of illicit merchandise or non-drug contraband in commercial cargo shipments is lacking.

Most existing foreign criminal intelligence and information collection efforts are aimed at providing actionable information to intercept illegal drug shipments into the United States. For example, there are two federal interagency committees consisting of federal law enforcement agencies

and the intelligence community aimed at disrupting and dismantling major heroin and cocaine smuggling organizations operating out of Southeast and Southwest Asia, South and Central America, Mexico, and the Caribbean. These committees meet regularly to disseminate intelligence and coordinate joint investigations and operational matters.

The Office of Naval Intelligence's Civil Maritime Industry Group, Counterdrug Division, began providing improvised container targeting support, primarily to federal law enforcement agencies, in May 1998. Most of this effort supports Latin America drug operations. In 1997, international business and transportation industry paperwork was analyzed. It demonstrated relationships among people and organizations buying, selling, distributing, smuggling, manufacturing, planning, and using containerized cargo. Precursor chemicals bound for Colombian cocaine laboratories were profiled, identified, and located. The analysis of this information was subsequently disseminated to Customs, resulting in six seizures of more than 105 metric tons of precursor chemicals.

To help fill the gap in drug-smuggling intelligence by commercial cargo and conveyances along the Southwest border, Customs instituted Intelligence Collection and Analysis Teams. Based on the Southwest border model, these teams have been instituted at the Ports of Los Angeles, New York/New Jersey, Miami, and San Juan. They are multidiscipline, tactical intelligence units whose sole responsibility is to produce actionable, tactical intelligence on the movements of drugs in and through the ports of entry. In some locations, they are also working on a wide range of criminal issues including stolen vehicles, illegal weapons smuggling, and money laundering. Customs Intelligence Collection and Analysis Teams produce intelligence reports for targeting and investigative leads on a daily basis.

While these programs have been effective against drug smuggling activities, they may not be as effective against smuggling chlorofluorocarbons, trademarked and copyrighted products, and other non-drug contraband because many law enforcement agencies stationed abroad collect very little intelligence and information necessary to interdict contraband in the United States. Therefore, the activities of U.S. government law enforcement personnel stationed abroad must be intensified to remedy this weakness.

Finally, intelligence resources must be used more effectively to provide focused targeting on suspect non-drug shipments and violators, and intelligence collected by domestic law enforcement must be disseminated more widely. Many federal agencies maintain data on violators and the types of violations they have found. Illegal activity such as smuggling may represent violations of more than one agency's laws and regulations, with each agency tracking those activities independently. With the exception of interagency task force operations, very little of this information is routinely exchanged. Interagency sharing of violation histories might help in targeting inspection activities and in fostering joint agency operations. Sharing intelligence would also help agencies identify the smuggling techniques used to circumvent U.S. laws.

Federal Intelligence and Law Enforcement Agencies

The following are brief accounts of a number of current federal agency capabilities for developing and processing information related to targeting and interdiction of contraband in commercial cargo and other seaport crime. Discussion of some agencies and programs has been omitted because of security classification constraints on making the information available.

The Intelligence Community

The Director of Central Intelligence serves simultaneously as Director of the Central Intelligence Agency and as the leader of the Intelligence Community. The Intelligence Community refers in the aggregate to those Executive Branch agencies and organizations that conduct the variety of intelligence activities that make up the total U.S. national intelligence effort. The Community includes the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; offices within the Department of Defense for collection of specialized national foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the Department of State; Army, Navy, and Air Force intelligence; the Federal Bureau of Investigation; the Department of the Treasury; and the Department of Energy. Members of the Intelligence Community advise the Director of Central Intelligence through representation on a number of specialized committees that deal with intelligence matters of common concern. Chief among these are the National Foreign Intelligence Board and the Intelligence Community Executive Committee, chaired by the Director of Central Intelligence.

Director of Central Intelligence Crime and Narcotics Center

The Central Intelligence Agency's Directorate of Intelligence houses the Director of Central Intelligence Crime and Narcotics Center, which monitors, assesses, and disseminates information on international narcotics trafficking and international organized crime to policymakers and the law enforcement community. The Counter-Narcotics Center was established in April 1989, and its mission and name were expanded to include international organized crime in 1994. The Center is staffed with representatives from all Directorates within the Agency and includes direct participation of most Intelligence Community, counter-crime, and counter-narcotics law enforcement and policy agencies.

Defense Intelligence Agency Office for Counterdrug Analysis

The Defense Intelligence Agency's Office for Counterdrug Analysis coordinates the Agency's intelligence support to the counterdrug intelligence and law enforcement communities. It also provides strategic and operational intelligence support to Department of Defense military commands and law enforcement agencies. Primary areas of emphasis include coordinating activities of overseas counterdrug representatives and supporting overseas country teams, developing intelligence support packages for country teams and host nations, exploiting captured documents, preparing drug trafficking organization profiles, managing the Counterdrug Intelligence Data System, and coordinating the interagency assessment of cocaine movement.

Bureau of Alcohol, Tobacco, and Firearms

The Bureau of Alcohol, Tobacco, and Firearms collects information on commercial seaports to support specific investigations of firearms trafficking patterns and alcohol and tobacco diversion. The information is disseminated to the Bureau's field divisions and field offices for action with investigative cases. Information is collected on foreign businesses or persons that ship goods in cargo containers if they are believed to be involved in firearms trafficking or alcohol and tobacco diversion. The Bureau receives national-level intelligence at the headquarters intelligence division. A mechanism is in place to task the intelligence community on specific collection requirements. It has been used frequently, and the information received has been extremely useful in the investigations. In a number of instances, intelligence was used as lead information to initiate an investigation.

Customs

Customs collects information on imports in order to appraise and classify merchandise and ensure compliance with laws and regulations. Customs also uses advance manifest information to conduct risk assessments on cargo. Customs has long collected intelligence on the movement of drugs and other contraband via intermodal containers, and it has been at the forefront of the effort by the intelligence community and other federal law enforcement agencies to encourage the development of more intelligence related to cross-border smuggling. Customs develops its own intelligence from investigations and informants. This intelligence is specific to Customs' drug interdiction mission, and it focuses on specific intelligence that is needed to target high-risk modes of conveyance, intermodal containers, traffickers, and smuggling methods. Customs has established a series of multidiscipline Intelligence Collection and Analysis Teams at most major ports of entry, whose core responsibilities are to collect all-source intelligence, focusing on conveyances, intermodal containers, traffickers, and smuggling methods.

Customs receives national-level intelligence from a variety of sources, including other federal law enforcement agencies and the U.S. Intelligence Community. This information runs the gamut from narcotics-related intelligence to terrorism and trade crime information. National-level intelligence is critical to the mission of the Customs Service and constitutes a major component of both its investigative and interdiction activities. National-level intelligence is widely disseminated to Customs field units, including inspection, investigative, and intelligence groups. Typically, national-level intelligence is received in a classified format. This information is usually sanitized and, in some cases, declassified. Sanitized intelligence may be entered into the Treasury Enforcement Communications System, Customs' national database.

Customs, through Treasury, makes its requirements for intelligence known through formal mechanisms such as the National Human Intelligence Requirement Collection Process. Customs also directly tasks the Intelligence Community for assistance through requests for information or special intelligence collection requirements. National-level information frequently contributes to ongoing investigations. Investigative leads, consisting of various kinds of information, are used by all Customs field investigative units, and they contribute to further targeting of command-and-control centers of organized criminal groups. Warehouses, stash sites, crossing points, vehicle information, and identification of members of drug groups are examples of information that is passed on a routine basis and that enhances investigations. Drug groups and organizations are frequently targeted based on this information, and overall the information contributes to both interdiction and investigations.

Commerce

Export Enforcement collects information relating to sensitive dual-use exports in order to enforce U.S. export control laws in place to protect sensitive American products from being diverted to countries developing weapons of mass destruction, terrorists, and others working counter to the interests of the United States. This information is disseminated to Enforcement's eight field offices for action and investigation. Export Enforcement develops intelligence from its own investigations and informants. It also receives national-level intelligence from a variety of sources, including other federal law enforcement agencies and the U.S. intelligence community. This information is specifically related to domestic and foreign efforts to circumvent U.S. export control laws. Export Enforcement concentrates on using intelligence to target diverters and identify foreign procurement networks seeking U.S. dual-use goods, front companies, and brokers.

Coast Guard

The Coast Guard has many missions. With the end of the Cold War and the increase in asymmetric threats that may be moved by maritime means—such as terrorism, and smuggling of narcotics, aliens, weapons of mass destruction, and other materials—the Coast Guard has seen its own role in the national security area grow. In this new environment, Coast Guard intelligence interaction with the Department of Defense and the intelligence community has dramatically increased. This relationship recognizes the Coast Guard's unique status as both a federal law enforcement agency and one of the five armed services. Only the Coast Guard can exploit the national foreign intelligence community as a military service, while at the same time enforcing U.S laws. Intelligence supports all of the Coast Guard's primary mission areas, including interdiction of drugs and illegal aliens, preservation of living marine resources, and protection of the marine environment. It also supports expanding missions such as port security, countering the entry of weapons of mass destruction, and homeland security.

The primary goal of Coast Guard intelligence is to leverage, not duplicate, the work of other intelligence agencies. To enable this, Coast Guard Intelligence Information Resources Management systems are connected with law enforcement, defense, and intelligence community systems. Its secure computer system, the Coast Guard Intelligence Support System, is interoperable with the Defense Department's Joint Deployable Intelligence Support System. The Coast Guard is able to communicate with the intelligence community via the Joint Worldwide Intelligence Communication Systems circuit and the Secret Internet Protocol Router Network. The Coast Guard also maintains the Law Enforcement Information System database on suspect vessels, and it has access to several marine safety databases that assist in tracking suspect vessels.

The Coast Guard has detailed officers to several major intelligence activities, including the Central Intelligence Agency, the El Paso Intelligence Center, the National Drug Intelligence Center, the Defense Intelligence Agency, the National Security Agency, the Joint Intelligence Command Pacific, and the Joint Inter-Agency Task Forces East and West. Additionally, the Coast Guard maintains accredited Coast Guard attachés in Colombia, Mexico, the Dominican Republic, and Venezuela, and soon Panama. The Coast Guard also maintains close working relationships with the respective High Intensity Drug Trafficking Areas and Organized Crime Drug Enforcement Task Forces.

The Coast Guard routinely receives intelligence from throughout the law enforcement and intelligence community. This intelligence is essential to accomplishment of the Coast Guard's mission. While constrained at present by assigned resources, the process is capable of expansion to support operations directed at a variety of emerging maritime threats.

Drug Enforcement Administration

The Drug Enforcement Administration's Intelligence Division runs several Special Field Intelligence Programs that target commercial seaports in South America. These efforts focus on drug smuggling operations in ports in a number of source countries, targeting drug shipments concealed in containerized cargo destined for the United States. Information collected under these programs is passed to the El Paso Intelligence Center, or directly to other law enforcement agencies as appropriate.

The El Paso Intelligence Center is a 24-hour tactical drug intelligence center under the Drug Enforcement Administration. Personnel from 14 federal agencies work together to provide information to field entities for interdiction and investigative purposes.

Immigration and Naturalization Service

The Immigration and Naturalization Service is a law enforcement agency. Although it collects intelligence and other information relating to seaports, shipping, and other maritime data, this information collection is collateral to Immigration's primary enforcement responsibilities. Information relating to cargo container shipments is not collected routinely or systematically. Immigration collects information on foreign businesses or persons that ship consumer goods in cargo containers only insofar as it is relevant in the regulation of aliens and foreign businesses operating in the United States.

Immigration collects information on alien smuggling activity that takes place on commercial shipping vessels. The El Paso Intelligence Center's Alien Intelligence Unit collects and analyzes reporting on alien smuggling organizations that operate worldwide. This unit has developed more than 2,000 alien smuggler target intelligence files. Immigration maintains intelligence information on alien smuggling that arrives via commercial vessels as well as by private vessels or, in fact, via land or air. As relevant, this information is shared with the Customs Service or the Coast Guard. It is shared with state or local agencies only in the context of specific ongoing joint operations. Intelligence on alien smuggling is the only intelligence that is collected systematically, as narcotics interdiction is secondary to Immigration's primary mission.

The Immigration and Naturalization Service receives national-level security information at the headquarters level and through the Joint Terrorism Task Forces at the local district office level. Some classified information is sanitized and then entered into lookout systems, which are not classified but which operate as limited official use–law enforcement-sensitive. Immigration participates in the formation of human intelligence requirements with other law enforcement agencies and it can propose collection requirements, but it does not task the intelligence community directly. Some information received on alien smuggling has been valuable for lead purposes. The timeliness of information received has varied greatly from case to case. However, most of this intelligence is not specific enough with regard to time, locations, or involved individuals to prompt Immigration enforcement action. In general, actionable intelligence has been generated internally rather than received from other sources.

Office of Naval Intelligence

The Office of Naval Intelligence has a Counterdrug Division that supports requests for information on high-interest suspect drug trafficking vessels or maritime-related items from the Department of Defense and various law enforcement agencies. The Civil Maritime Analysis Department has begun a project that analyzes foreign businesses and is capable of some network profiling. An expansion of this intelligence model to include communications intelligence, human intelligence, and document exploitation could provide useful information for container targeting. The Small Ships Database contains information on nearly 6,000 vessels under 100 gross tons and more than 28,000 associated vessel movements. The Office of Naval Intelligence, in conjunction with the Coast Guard Intelligence Coordination Center, has loaded more than 5,000 images of small vessels in the AMIDSHIPS database, which is accessible to the counterdrug community via SEALINK.

National Reconnaissance Office

The Department of Defense's National Reconnaissance Office coordinates the collection of national security-related information via space-based surveillance systems. The Office is currently develop-

ing a Law Enforcement Application Program (LEAP) to better support the information needs of law enforcement agencies, and to develop a legal framework for administrative and operational processes for disseminating relevant information to appropriate agencies. The primary goal is to develop an organized, systematic approach to exploring the utility of space-based reconnaissance systems for responsive support of federal law enforcement agencies' operational needs.

National Drug Intelligence Center

The National Drug Intelligence Center is an independent component of the Department of Justice. It is responsible for providing counterdrug agencies with timely, multisource assessments on drug trafficking organizations. The information is specific enough to assist law enforcement agencies with their investigative initiatives, yet general enough to provide strategic value to the overall community. The Center explores open-source materials and keeps up with the activities of the counterdrug community in search of emerging trends and patterns. It uses information from federal, state, and local law enforcement agencies, coupled with related foreign assessments from the intelligence community, to accurately reflect the global threat posed by drug trafficking. The Center produces the *National Drug Threat Assessment,* a timely, predictive intelligence report for policymakers and counterdrug executives on the threat of drugs, gangs, and violence. It synthesizes the views of local, state, regional, and federal agencies to produce a comprehensive picture of this national threat. Based on specific threats identified, the National Drug Intelligence Center produces additional intelligence reports consisting of predictions, strategic estimates, organizational assessments, and baseline studies. It publishes the *National Drug Intelligence Digest,* a macro-level assessment of emerging issues and trends of concern to the law enforcement community, which highlights changes, patterns, and trends on the domestic drug front.

Joint Maritime Information Element

The Joint Maritime Information Element (JMIE) originated in the mid-1980s when a group of federal agencies with important maritime security, safety, regulatory, and enforcement responsibilities sought to improve ways to share information and data. Today, it is a consortium of agencies from the intelligence, law enforcement, and defense communities. It provides member agency analysts ready access to multisource maritime data and enables agile processing and correlation of the data to meet their information requirements. Pooling maritime-related information into one central database and developing an automated information-handling system enable users to query other agency data sources, correlate results, and gain timely and improved information. The database contains information from multiple sources on merchant ships, cargoes, fishing and research vessels, and pleasure craft.

The Joint Maritime Information Element mission is to improve the availability of maritime information to member agencies and to develop synergy among the members in support of their maritime missions. Members of the consortium are the Central Intelligence Agency, Coast Guard, Customs, Defense Intelligence Agency, Drug Enforcement Administration, Department of Energy, Immigration and Naturalization Service, Maritime Administration, Military Sealift Command, National Security Agency, Office of National Drug Control Policy, Office of Naval Intelligence, and Department of State. The Joint Maritime Information Element is under joint Coast Guard and Navy management, and is accessible on the SECRET Internet Protocol Routing Network (SIPRNET).

Threat Dissemination

One of the key concerns in information-sharing is that intelligence on terrorist threats to port facilities, maritime transportation systems, and other critical port infrastructure must reach appropriate personnel, both within the law enforcement agencies that must prevent and respond to terrorist acts and within the private sector that owns and operates the vast majority of that infrastructure. The following section describes federal agency efforts to disseminate terrorist threat information to appropriate law enforcement agencies, port authorities, private sector vessel and facility operators, and the traveling public. This section also compares threat dissemination procedures at airports and seaports.

Federal Bureau of Investigation

The Federal Bureau of Investigation is the lead federal law enforcement agency for combating terrorism within the United States. In addition, it has jurisdiction overseas when a U.S. national is murdered, assaulted, or taken hostage by terrorists, or when certain U.S. interests are attacked. The FBI has established the National Threat Warning System to ensure that vital information on domestic terrorism reaches the members of the U.S. counter-terrorism community and law enforcement community for use in responding to terrorist threats. The major threat warning system recipients are the Departments of State, Defense, Treasury, Energy, and Transportation; the Central Intelligence Agency; National Security Agency; Environmental Protection Agency; Customs Service; Secret Service; Bureau of Alcohol, Tobacco, and Firearms; Internal Revenue Service; Immigration and Naturalization Service; Bureau of Prisons; Drug Enforcement Administration; Federal Aviation Administration; Coast Guard; Naval Criminal Investigative Service; Air Force Office of Special Investigations, Army; and White House Situation Room.

The FBI uses several means to disseminate threat information. If the information warrants broad dissemination, unclassified messages are quickly transmitted to state and local law enforcement agencies nationwide over the National Law Enforcement Telecommunications System. Information that is less urgent is communicated through the Law Enforcement On-line system. For the private sector, "Awareness of National Security Issues and Response Warnings" are issued to as many as 5,000 companies in the U.S. business community. These messages are transmitted as assessments, advisories, or alerts. They include criminal threat information such as product tampering, extortion, computer crimes, and criminal hijacking. In addition, the National Threat Warning System provides a mechanism for public threat notification when appropriate.

The FBI's field offices routinely share information through their ongoing working relationships with state and local law enforcement agencies. To strengthen these existing relationships and improve communication about terrorism issues, the FBI created Joint Terrorism Task Forces (described in detail in Chapter 4). Currently located in 26 metropolitan areas, they are composed of representatives from the FBI, federal law enforcement agencies such as Alcohol, Tobacco and Firearms, Immigration, and the Naval Criminal Investigative Service, and officials from state and local law enforcement agencies. Members of the Task Forces work together, usually on a full-time basis, to gather, analyze, and disseminate intelligence and investigate terrorist activity.

In addition to Joint Terrorism Task Forces, the FBI has established regional terrorism task forces to serve several rural states that have common terrorism concerns. These task forces share terrorism-related intelligence and sponsor regional terrorism conferences to train local law enforcement agencies about the terrorism threat in their region. These working

arrangements not only improve the flow of information from federal intelligence agencies to localities, but they allow federal agencies to obtain intelligence from local sources.

Department of State

U.S. government policy requires the dissemination of information to the general public about specific and credible overseas terrorist threats that cannot be countered. When the threat applies to the general public, there is no double standard between information available to government officials and to private citizens. When terrorist threat information is received, the State Department's Office of the Coordinator for Counterterrorism coordinates the interagency effort to determine if public dissemination is appropriate. Depending on the nature of the threat, public dissemination will be effected by the issuance of a travel advisory (or revision of an existing advisory) or a public statement or press briefing by the State Department. A public announcement or travel advisory will generally include recommended actions to reduce risk, such as deferring travel to a particular country.

Department of Defense

The Defense Intelligence Agency provides terrorist warning and analysis support to the Joint Staff, Office of the Secretary of Defense, and to the unified commands. It provides prompt dissemination of intelligence information on terrorist threats, including specific warning of threats against service personnel and their family members, facilities, and other Defense Department assets. The Defense Intelligence Agency is the focal point within the Department for data and information pertaining to domestic and foreign terrorist threats to Defense Department personnel. In addition, it provides support to policymakers and programs, counterterrorism collection, operations, and the investigation communities.

Department of Defense terrorist threat warnings are accomplished using two mechanisms. The intelligence community system issues fully coordinated terrorist threat alerts and advisories. The services have the opportunity to comment on proposed warnings, and direct their responses through the Defense Intelligence Agency. The executive coordinator of the Community Counterterrorism Board is responsible for coordinating threat warnings outside the United States, and the Federal Bureau of Investigation is responsible for coordinating and issuing intelligence community warnings for domestic threats. The second system is the Defense Indications and Warning System, in which members at any level may initiate unilateral threat warnings, called terrorism warning reports. Warnings within the Department generally stay within the system and are primarily for use of Defense Department activities. Before a warning is issued, the Community Counterterrorism Board is consulted to determine whether the national community will issue an advisory or an alert.

Warnings are issued when a specific target and timing exist or when analysts have determined that sufficient information indicates that U.S. personnel, facilities, or interests, are being targeted for attack. The purpose is to identify threat information to prevent the compromise of deployed U.S. military forces to espionage, foreign intelligence collection, sabotage, terrorism, and assassination. Commanders in Chief of the combatant commands (CINCs) are responsible for reviewing the antiterrorism force protection status of all military activities, including Department of Defense contracting activities, within their geographic area of responsibility.

Commanders in Chief and military base commanders issue Threat Conditions (THREATCONs). These are based on the perception of security threat to their facilities, and are not necessarily tied to the terrorist threat level. Threat Conditions describe the progressive level of a terrorist

threat to all U.S. military facilities and personnel. They are recommended security measures designed to ease interservice coordination and support of U.S. military antiterrorism activities. Once a Threat Condition is declared, the selected security measures are implemented immediately.

- THREATCON NORMAL applies when a general threat of possible terrorist activity exists but warrants only a routine security posture.
- THREATCON ALPHA applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which is unpredictable, and circumstances do not justify full implementation of THREATCON BRAVO.
- THREATCON BRAVO applies when an increased and more predictable threat of terrorist activity exists.
- THREATCON CHARLIE applies when an incident occurs or intelligence is received indicating that some form of terrorist action against personnel and facilities is imminent.
- THREATCON DELTA applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely.

Department of Transportation

The Aviation Security Act of 1990 established the Office of Intelligence and Security within the Department of Transportation, and made the Director accountable for overseeing the development of policies, strategies, and plans for dealing with threats to transportation security. The Director serves as the department's primary security policy official and liaison with Transportation's operating agencies, other federal agencies, the transportation industry, and the intelligence and law enforcement communities on transportation security matters. The Office of Intelligence and Security coordinates and disseminates terrorist threat information to the Department's operating administrations for distribution to their regional and field offices and to law enforcement and transportation industry contacts. This information is distributed in the form of Transportation Security Information Reports. These reports are intended to advise recipients of emerging security threats, the potential for near-term terrorist attacks, or other security-related information of interest to transportation security personnel. A threat is defined as any indication of planned violence against U.S. persons, transportation facilities and infrastructures, including computer networks. A threat can originate from individuals, terrorist groups, or other criminal elements. The reports are produced in an unclassified format, using both classified and unclassified information available from a number of sources. Department of Transportation operating administrations transmit the reports to regional and field offices, law enforcement officials, and industry security contacts, and encourage law enforcement and security personnel to take measures to enhance security and to reduce the vulnerability of the transportation system to the reported threat.

Coast Guard

The Coast Guard disseminates threat information affecting the marine transportation industry to a variety of private sector commercial interests. Threat information is generally received by the Assistant Commandant for Marine Safety and Environmental Protection at Coast Guard headquarters from the Department of Transportation's Office of Intelligence and Security or through the Coast Guard Intelligence Coordination Center. This information is forwarded in the form of threat advisories via Coast Guard district offices to the Coast Guard Captain of the Port. Each Captain of the Port distributes the informa-

tion to port authorities, waterfront facility operators, shipping agents, vessel operators, and other local port stakeholders. This information is primarily distributed for private sector security personnel to act on voluntarily. However, the Captain of the Port may direct operators of vessels and waterfront facilities to implement enhanced security measures before continuing cargo or passenger operations.

Maritime Administration

The Maritime Administration disseminates threat information to operators of U.S.-flag and effective U.S.-controlled vessels (vessels owned by U.S. interests but flagged in a foreign nation). Maritime Administration advisories are forwarded from the Office of National Security Plans to regional offices, where they are distributed to U.S. shipping companies and port authorities. Information is also distributed through the Office of Ship Operations in the form of Anti-Shipping Activity Messages. The Department of Defense's National Imagery and Mapping Agency, in carrying out its mission to produce Notices to Mariners, has developed an Automated Notice to Mariners System containing information on navigation safety. The database provides for remote queries that the agency makes available to the entire maritime community through the Navigation Information Network. The Anti-Shipping Activity Message file is available from this database as well as from the Maritime Administration's Web site.

Threat Dissemination at Airports vs. Seaports

It may be useful to compare threat dissemination procedures for airports, which operate with a regulatory scheme, with those in the seaport environment, which depend primarily on cooperation between the federal government and the private sector. The Federal Aviation Administration has in place a systematic process for disseminating threat information to airport and airline security personnel. Threat information is gathered and vetted by the headquarters Office of Civil Aviation Security. If the information is determined to represent a valid threat to security, it is transmitted in one of two forms, Information Circulars or Security Directives. Information Circulars provide threat information to the private sector that may be acted upon voluntarily, with airport and airline operators enhancing security measures at their discretion. Security Directives specify mandatory security measures. In either form, threat information is passed from the Office of Civil Aviation Security to Federal Aviation Administration regional offices and then to civil aviation security field offices. The information is then forwarded to individual airport security coordinators directly or, in the case of the largest (Category X) airports, via the federal security manager assigned there. For airlines, threat information is passed to the air carrier's ground security coordinator via the Federal Aviation Administration's principal security inspector at the field office. Procedures for disseminating threat information and responsibilities for implementing security measures are specified in regulations stemming from the Aviation Security Act of 1990.

Remaining Threat Dissemination Questions at Seaports

As the descriptions above indicate, multiple federal agencies, each targeting different customers, distribute terrorist threat information. These processes appear to be working well, with end users gaining access to threat information through the most appropriate channels. Therefore, there appears to be no need to centralize the distribution of threat information within a single federal agency, or to incorporate threat dissemination procedures for seaports into regulation, as is the case for aviation security. However, some issues persist.

Although management of private sector companies may receive threat information directly from federal agencies or indirectly

through port authorities or local maritime trade associations, that information may not always reach the security personnel who must implement enhanced security measures. In many cases, this is a failure of internal communication within the private sector. Increasing the awareness of terrorist threats among port facilities and vessel operators, and expanding the availability of threat information from government sources through training, outreach, and public/private interagency forums, such as local port security committees, would do much to alleviate this problem.

Threat information assembled by government agencies is often classified for reasons of national security. Few persons among the target audience for this information, especially within the private sector, possess the requisite security clearances to receive it. Therefore, threat information must be sanitized so that it can be presented in an unclassified form while protecting the sources of that information and methods of collecting it. Sanitized threat warnings, standing alone, may lack sufficient detail to prompt action by local law enforcement and private sector security personnel. Developing good working relationships among port-level federal agency personnel, local law enforcement personnel, and private sector stakeholders can help to build confidence in the messenger and thus the message, and enhance the credibility of such warnings.

Managing Seaport Information

Seaports are a key confluence in the transportation system. They present a complex nexus of vessel movements, passenger lists, and cargo manifests where significant information about the nature, volume, and location of intermodal exchanges resides. Integrating and managing this information is crucial to maintaining control of our maritime borders. As barriers to trade and travel are reduced and volumes of international cargo and passengers grow, opportunities for criminals to exploit the commercial transportation system also increase. Pertinent information is needed to detect, intercept, and prevent terrorism and criminal activity within seaports. Existing information about the movement of vessels, people, and cargo is not integrated, nor is it readily available to responsible security organizations.

Law enforcement and inspection agencies must identify and intercept illegitimate activities hidden in an environment of similar-looking legitimate activities. Separating the “bad” from a sea of “good” requires real-time knowledge of vessels, people, and cargo approaching, moving through, and departing a seaport. Greater knowledge of cross-border flows of people and goods will facilitate detection of criminal and terrorist activity. Improved targeting information made readily available to all interested inspection and law enforcement agencies will permit them to focus their efforts on cargo, persons, and vessels that present the highest risk to security while reducing random inspections that increase disruptions to commerce and result in costly delays.

In addition, the maritime industry needs to be aware of the location and status of vessels and cargo, and it must manage a variety of information desired by its customers and demanded by federal agencies. A variety of information systems exist, in both the public and private sectors, for managing this information. These include automated systems for processing and clearing import and export cargo; asset management systems to locate and track vehicles and containers; security systems to monitor vehicles, containers, and cargo in transit or storage; vessel traffic systems to track the position and movement of vessels; and real-time weather, oceanographic, and vessel identification systems for safe navigation.

An integrated port information system could satisfy the need for information brokerage for private sector business activities while supplying critical decision making support for government agencies. The value of such a system has previously been identified in *An Assessment of the U.S. Marine Transportation System,* a report to Congress submitted by the Secretary of Transportation, and also in *Turning to the Sea: America's Ocean Future,* a report to the President jointly prepared by the Secretaries of Commerce and the Navy.

Investments in the area of upgrading and integrating seaport information systems should receive high priority consideration in the budget development process. A variety of initiatives for upgrading information systems (including automated systems for processing cargo and passengers) are underway throughout the federal government. Integrating these systems in a deliberate fashion will enable the nation to reap current benefits while setting the stage for future assimilation of vessel and cargo tracking sensor technology. Integrating this information will provide "one-stop shopping" for a total operational picture of port activities and will enable security agencies to make valid risk-based targeting decisions for allocating scarce resources.

Findings and Recommendation

Finding 18. Information about the movement of vessels, people, and cargo within seaports is not integrated, nor is it always readily available to government and private sector security organizations responsible for detecting, intercepting, and preventing terrorism and other criminal activity.

Recommendation 18. Improve information (including intelligence) collection, integration, and dissemination at the seaports by proceeding as follows:

- The Coast Guard should work with relevant agencies to coordinate development of an integrated, real-time information system for tracking the movement of vessels (including cargo and personnel) within the seaport environment. This system would be available for use by relevant law enforcement and inspection agencies in crime prevention and security efforts.
- Law enforcement agencies should develop specific collection requirements for foreign intelligence collection efforts concerning the illicit movement of merchandise and contraband in commercial cargo through seaports.
- The Central Intelligence Agency and other national intelligence agencies should increase foreign intelligence collection efforts aimed at providing specific, actionable information about those international criminal activities affecting seaports that have been identified as national security threats to the United States (e.g., drug trafficking and proliferation of weapons of mass destruction).
- Law enforcement agencies should work together to ensure that they have an effective mechanism to process and share intelligence at the seaport level as appropriate.

Chapter 8: International Considerations

Most of the issues described in previous chapters have an international component, be it trade, terrorism, international passengers or crewmembers, or cargo. International cooperation can be critical in addressing many of these issues.

Issues that confront the United States in the international arena include the following:

- Economic globalization is compressing reaction time and blurring national borders.
- International criminal and terrorist threats are constantly changing and adapting to law enforcement capabilities. Today's communications and integrated intelligence systems lack the sophistication to support real-time monitoring of vessels, people, and cargo movements.
- The wide-ranging state of development, differing port operation management structures, and amount of resources available to the seaports of the world present a formidable challenge to developing a coordinated approach to the detection of crime and establishing international seaport security standards.

International commerce has changed dramatically since the end of the Cold War. Globalization and the liberalization of trade practices have resulted in fewer impediments to trade and an increase in the flow of goods, most of which are transported by sea. Advances in technology and communications have changed the way companies conduct business. More companies have become global in nature. International competition, open markets, and the dropping of trade barriers contribute to the selection of goods available to U.S. consumers and producers. Developed nations like the United States are increasingly dependent on foreign markets to produce goods through cheaper manufacturing costs. In addition, exports are playing a key role in strengthening the U.S. economy and national security. Exports are responsible for creating 12 million jobs in the United States. Exports are providing high tech firms with the disposable capital to invest in research and development and bring new products to market, thus ensuring that the U.S. military has the most advanced technology to draw upon.

At the same time, the influx of goods through U.S. ports provides a venue for the introduction of a host of transnational threats into the U.S. infrastructure. These include drugs, weapons (both conventional and weapons of mass destruction), and illegal migrants. Further, the nexus of transportation modes, as well as the concentration of passengers, high-value cargo, and hazardous materials in seaports, make them potential targets for terrorist attacks.

The position of the United States as a world power and our dependence on foreign trading partners makes this country vulnerable. Threats can come from an adversary, a rogue state, an organized criminal element, or an individual. Instability in regions where governmental regimes are changing may increase the threat. The security of domestic ports is affected by the security of ports at the originating and transit points of the shipping "logistics chain."

Despite the status of the United States as a world leader, the susceptibility of U.S. ports to the repercussions of lax security

in foreign ports makes international port security engagement a priority. The United States must seek the cooperation of its trading partners in eliminating crime, and it should lead the world in developing international port security standards and conducting training to facilitate the implementation of those standards.

The activities of international organized crime adversely affect the economic competitiveness of legitimate open market commerce and deter trade and investment. The billions of dollars derived from illicit enterprises enable organized crime groups to compromise and penetrate commercial markets and acquire legitimate companies. This further equips them with the instruments to advance their criminal enterprises and obfuscate their operations in the process. The effects can discourage the commercial initiative of U.S. business interests operating overseas. The most powerful criminal syndicates may be capable of achieving substantial influence or even monopolistic control over critical sectors of the national economy of some countries. The result may diminish multilateral efforts to promote more cooperative solutions to global trade problems and may prevent credible economic systems from being instituted.

International organized crime groups are taking full advantage of the growth in sophisticated global commerce, transportation, communication, and financial links to perpetrate cargo crimes involving smuggling, cargo theft, and money laundering. Criminal exploitation of the maritime trade corridors places in jeopardy the international commerce of the United States and its global economic alliance. U.S.-flag ocean carriers call on ports in nearly every country, and cargoes owned by U.S. interests may be embarked on ocean vessels of any flag or in any port worldwide. U.S. commercial maritime interests, therefore, can be jeopardized worldwide by a broad range of organized criminal activities, adversely affecting their competitiveness.

Unconstrained by borders or national sovereignty, international organized crime groups are operating transnationally and deriving billions of dollars from a wide range of cargo crimes. Among the most lucrative types of cargo crime is cargo theft itself and the smuggling of drugs, alien migrants, stolen goods including automobiles, contraband merchandise, and illicit currency shipments. Levels of containerized cargo volumes are forecasted to increase significantly. This will create more opportunities for cargo crime while lowering the statistical risk of detection and interdiction.

Ports as Marine Intermodal Choke Points

International maritime trade corridors consist of three main logistical components—ports, ocean vessels, and the landside modes of transport. Functioning as pivotal nodes in a system of trade routes, the seaports provide intermodal interface to the international maritime shipping cycle. Among the trade segments engaged in marine intermodal business transactions are, for example, ocean and land transporters, shippers, freight consolidators and forwarders, financial institutions, warehousers, labor unions, and the security departments of all parties involved.

Consequently, seaports and the freight movements through their landside accesses are viewed by cargo crime groups as marine intermodal choke points of commerce. Improved port and cargo security, therefore, is central to all efforts by government and industry to reduce criminal exploitation of commerce transported in the international maritime trade corridors.

International Crime Control Strategy

The Strategy, issued by the White House in May 1998, was developed through a coordinated process involving all relevant

federal agencies intended to improve U.S. government efforts to combat international organized crime and is based on Presidential Decision Directive 42, which was issued on October 21, 1995. This directive aims to improve international anti-crime efforts by strengthening the rule of law, and by fostering democracy, free markets, and human rights. The directive ordered executive branch agencies of the U.S. government to: (1) increase the priority and resources devoted to countering international crime; (2) achieve greater effectiveness and synergy by improving internal coordination; (3) work more closely with other governments to develop a global response to this threat; and (4) use aggressively and creatively all legal means available to combat international crime.

The Strategy is a plan of action. It complements other crime control documents, such as the National Drug Control Strategy and Presidential Decision Directives on, for example, alien smuggling (Directive 9) and counterterrorism (Directive 62). The Crime Strategy is intended to provide a framework for integrating all facets of the federal response to the direct and immediate threat international crime presents to the national security interests of the United States. This Strategy is intended to be dynamic, adaptable, and sufficiently flexible to enable its extrapolation into tailored applications and subsidiary strategies, including one specifically tailored to address international crime's impact on port and cargo security.

The Strategy goals and objectives address many specific issues and provide broad guidance for many others. This Strategy also includes numerous programs and initiatives that serve as a blueprint for an effective, long-term attack on the international crime problem. The goals are listed in Appendix C.

Marine Transportation System Task Force

The Marine Transportation System Task Force—a federal interagency and private sector assessment of the U.S. marine transportation system—reported to Congress in 1999 that the United States must be able to detect, intercept, and respond to threats to the Marine Transportation System as far offshore as possible. The report also included findings that overseas ports serve as primary entry points in the system for U.S.-bound cargoes and people. Because the origin of much of the cargo that moves through the Marine Transportation System lies well beyond U.S. borders, more effective international cooperation is needed to establish and police security standards at overseas ports in our international trade corridors. Improving foreign seaport security capabilities will reduce the risk that contraband or terrorists will find their way into the United States.

The Marine Transportation System Task Force therefore recommended, for example: (1) the development of a strategy and process for advancing U.S. operating guidelines and minimum security standards on an international basis; (2) providing intelligence and training to improve international oversight of the global maritime infrastructure; and (3) support of the Interagency Commission on Crime and Security in U.S. Seaports.

In addition, the Task Force specified that efforts should be incorporated into several ongoing interagency and public/private sector efforts, including the Interdiction Committee and the following Customs Service initiatives: the Carrier Initiative Program, the Americas Counter-Smuggling Initiative, and the Business Anti-Smuggling Coalition. The improved capabilities of foreign seaport police and security personnel developed with—guidelines, standards, strategy, intelligence, and training—thus create multilateral operational benefits and improvements in the security of the international maritime trade corridors.

In its report the Task Force identified five strategic areas for action related to security: improving security awareness; improving transparency; ensuring qualified operators; forging stronger public/private partnerships; and strengthening international cooperation. These areas were studied by the Commission and are addressed in Appendix C of this report.

Presidential Decision Directive 63, *Protecting America's Critical Infrastructures*

This directive called for an effort to establish international cooperation as a means of protecting the U.S. infrastructure. The directive identifies several findings that are addressed by the Commission in Appendix C.

As it relates to seaport security, international cooperation has at least three key components:

- Cooperation (including the gathering and sharing of information).
- Training with respect to seaport operations and security.
- Standards for seaport security operations.

During the Commission's port visits, it became evident that these areas needed to be addressed on an international level. Many government agencies, including the FBI, Customs, and the Coast Guard, expressed the need for better information and cooperation from foreign countries that export to U.S. seaports. The Commission believes that cooperative engagement with this country's international trading partners is essential to effecting meaningful and lasting improvements to seaport crime and security.

U.S. seaports, as a critical infrastructure subset of the marine transportation system, are especially vulnerable to criminal or terrorist activities because of their scale, complexity, and pace of activity. As a nation that is both consumer and producer, the United States can expect that foreign trade in goods will continue to increase. The overwhelming bulk of this trade will flow through the nation's seaports. Increases in federal assets, including equipment, facilities, and personnel, at the seaports have not kept pace with the increases in trade volume. To accommodate increases in trade and still maintain an acceptable level of security and law enforcement at seaports will require new and innovative enforcement and security measures.

These measures will require increased cooperation with our international partners. As governments remove barriers to trade and travel, U.S. officials will need more advanced information on the cross-border flow of people and goods and on other maritime activities (such as vessel operations/schedules) in order to identify actual and potential threats.

U.S. Agencies' International Cooperation Programs

Many U.S. agencies, including the Coast Guard, the Maritime Administration, Customs, the FBI, the Department of State, the Department of Commerce, and the Environmental Protection Agency, have international programs and initiatives in place that relate to the key issues of cooperation, training, and standards. These programs may include deployments, foreign liaisons, attaches, advisory groups, and training for foreign nations.

Customs, the Coast Guard, Immigration, the Federal Law Enforcement Training Center, and the Maritime Administration have international port security training programs. The Maritime Administration coordinates with the Organization of American States to provide an inter-American port security training program funded through the Organization of American States. Utilizing instructors from Customs and personnel from two U.S. port authori-

ties, the Maritime Administration has developed a model training program in port security that provides training to 34 countries in the Western Hemisphere. This model could be used in other regions, including Africa, Eastern Europe, and Asia.

The Coast Guard provides assistance in many ways, such as training, maritime legal infrastructure assistance, port assessments, equipment sales or transfers, and operational cooperation. International training and technical assistance is coordinated by the Headquarters International Affairs Staff. Through its International Training Division, Coast Guard personnel are deployed worldwide to conduct training in all mission areas including Maritime Law Enforcement, Search and Rescue, Marine Environmental Protection, and Port Security. Foreign naval, coast guard, and police personnel are also brought to the United States for resident training. The Coast Guard assists nations with the development of effective maritime legal infrastructure through the Model Maritime Service Code project. This project, which is designed to assist partner nations in identifying and developing the necessary laws, regulations and policies to support a small naval service with roles and missions similar to those of the U.S. Coast Guard, provides the model for the legal authority necessary for the service to function effectively as a military service, a law enforcement organization, and a regulatory agency. In conjunction with Customs, the Coast Guard conducts foreign port assessments to make recommendations on the control of cargo shipments and to improve port security in order to reduce illegal drug shipments to the United States. Assessments have already been conducted in Peru, Ecuador, and Venezuela. In order to protect U.S. travelers from the risk of terrorism, Coast Guard personnel also perform vulnerability assessments for overseas cruise ship ports of call under the auspices of the Omnibus Diplomatic Security and Antiterrorism Act of 1986.

Under the auspices of the State Department and through its 38 Legal Attaché offices with regional responsibilities, the FBI conducts liaison activities with foreign law enforcement agencies and other foreign government officials. These Legal Attaché offices assist not only the FBI, but also other U.S. law enforcement agencies at all levels, in making contact with foreign law enforcement agencies in a cooperative fashion. FBI Legal Attaché offices also assist foreign law enforcement agencies in training matters.

The Environmental Protection Agency has been involved in coordinating between domestic and foreign law enforcement agencies to identify suspect shipments of waste destined for export. The project, Exodus Asia, has brought together a network of state and federal law enforcement agencies to focus on illegal shipments of waste from the United States to Asian nations.

The following are examples of recent international initiatives and programmatic activities of U.S. agencies in Latin America and the Caribbean. These international cooperative best practices contribute directly and collaterally toward substantially improving port and cargo security in the international maritime trade corridors of the Western Hemisphere.

Americas Counter Smuggling Initiative

Commercial transport has become the preferred method of smuggling for sophisticated trafficking organizations. In response, Customs developed the Americas Counter Smuggling Initiative as a priority undertaking designed to increase the effectiveness of countering drug smuggling via commercial cargo and conveyances. The Initiative is intended to strengthen cooperative regional efforts with the international trade community in Latin America. The objectives of the Initiative include increasing awareness of

contraband trafficking in the commercial environment and disrupting internal conspiracies. The Initiative focuses on each aspect of the commercial transportation process and offers a more comprehensive approach to dealing with this problem.

Business Anti-Smuggling Coalition

As part of its response to the problem of smuggling in commercial shipments, Customs established a business-led alliance in 1996, called the Business Anti-Smuggling Coalition. The Coalition is a response to Customs identification of commercial containerized cargo at seaports as its primary narcotics detection requirement. The Coalition is intended to significantly deter the use of legitimate commercial shipments as narcotic smuggling conveyances. It does so by examining the entire process of manufacturing, packaging, and shipping merchandise to the United States from foreign countries. The Coalition also addresses the growing problem of internal conspiracies at cargo handling and intermodal freight interchange points.

The Coalition assistance includes, for example, security site surveys, developing and implementing security programs, conducting post-seizure analysis in drug smuggling cases, and guidance on application and deployment of security technology. Assistance also includes development of information exchange relationships.

The Coalition is voluntary and without Customs-imposed mandates, relying instead on the international commercial industry to set standards. The Colombian government and the country's trade community have been especially cooperative with Customs in the Coalition initiatives overseas. It complements the Customs long-standing Sea Carrier Initiative Program, which emphasizes deterring narcotic smuggling onboard commercial ocean carriers.

Sea Carrier Initiative Program

Like the Business Anti-Smuggling Coalition, the Sea Carrier Initiative Program is a joint effort between commercial carriers and Customs. When it was established in 1984 to seek problem solving solutions to recurring problems, the concept was developed as an alternative to substantial fines and seizures of conveyances. Currently, approximately 2,870 sea carriers participate in the program. About 70 percent of these carriers are foreign-based. The program encourages the carriers to improve their port and cargo security practices to prevent drug smuggling via their conveyances.

Overseas Security Advisory Council

The Department of State, through its Overseas Security Advisory Council, interacts with industry on overseas security problems of mutual concern. More than 1,400 private-sector organizations participate in the Advisory Council's activities and receive information and guidance to defend against security threats such as terrorism, economic espionage, and organized crime. U.S. firms voluntarily submit accounts to the Advisory Council pertaining to security or crime incidents affecting their own or other U.S. overseas operations.

Inter-American Port Security Training Program

This Organization of American States initiative, managed by the Maritime Administration for the Organization of American States, provides port security training courses for commercial port authority police and security personnel. Participants in the training are from member countries of the Organization. This program was developed in cooperation with the Organization of American States Permanent Technical Committee on Ports. Port security is a major goal of the Organization, as expressed in its *Guidelines for an Inter-American Port Policy,* published in 1997.

In 1998, three subregional training courses were funded and conducted in Panama, Peru, and Barbados, in order to accommodate participation from Central and South America, and the Caribbean. The training teams consisted of instructors from U.S. commercial port authorities and the U.S. government. In 1995, training was conducted for Organization of American States countries, sponsored and organized by the Maritime Administration and the Organization of American States Inter-American Drug Abuse Control Commission.

Multilateral Cooperative Efforts

Several of the national strategies described in earlier chapters involve engagement by U.S. entities with international security efforts. An engagement policy is an assumption of the National Security Strategy, and is framed by the International Crime Control Strategy and the National Military Strategy. Key elements of strategy address international law enforcement cooperation, international crime and terrorism, and drug trafficking, all of which find a nexus in U.S. seaports. In addition, the National Drug Control Strategy involves international efforts to foster cooperation, improve international intelligence-gathering, and provide for interdiction operations to "shield America's sea frontiers from the drug threat."

To support the fight against drug smuggling, the United States has entered into several global, multilateral, subregional, and bilateral drug control accords. These range from the United Nations Drug Convention of 1988, to the Organization of American States Anti-Drug Strategy of 1996, to several Western Hemisphere multilateral accords, to bilateral maritime counterdrug agreements with 19 Caribbean and Central American nations.

The following are examples of multilateral cooperative efforts in which U.S. government agencies have demonstrated significant roles:

Caribbean/U.S. Summit Joint Committee on Justice and Security

This Joint Committee convenes annually to review the justice and security element of the plan of action agreed to by Caribbean heads of state, including President Clinton, at the May 1997 Bridgetown Summit. The 1999 meeting of the Joint Committee discussed progress made since the summit, which included increased cooperative maritime law enforcement efforts, substantial progress by the Caribbean Financial Action Task Force in money laundering investigations, and the ratification of a number of mutual legal assistance and extradition treaties. The 1999 meeting of the Joint Committee was co-chaired by Jamaica's Minister of National Security and Justice and the U.S. Assistant Secretary of State for International Narcotics and Law Enforcement Affairs.

The 1997 Caribbean/U.S. Summit

The agenda of the May 10, 1997, summit meeting between President Clinton and other Caribbean heads of state committed the United States to cooperation in formulating a plan of action linking security issues with the economic performance of island nations. The summit strategy formulated a new regional approach intended to integrate trade, economic, and environmental issues, with justice and security issues such as drug smuggling, money laundering, weapons trafficking, and strengthened criminal justice systems. The agenda recognized the important roles of trade and regional economic viability toward Caribbean nations becoming less exploited as transshipment points for drug smuggling and by other organized criminal activities.

The United States pledged to provide advice, technical assistance, and training in improving the security of manufacturing plants and the shipping cycle, and in combating customs-related corruption. The heads of the Caribbean states in turn agreed to engage transport companies and the private sector within their jurisdictions in a cooperative partnership. The intent is the development and adoption of security procedures and participation in programs that deter illegal access to and use of cargoes, commercial conveyances and associated equipment, and seaport and terminal facilities.

Organization of American States Technical Advisory Group on Port Security

The Maritime Administration serves as Chair and Secretariat of the Technical Advisory Group on Port Security of the Organization of American States Inter-American Committee on Ports, which has among its agenda: (1) developing a hemispheric approach to improving the security of the Inter-American maritime trade corridors; (2) developing a common port security strategy; (3) devising basic guidelines and minimum standards of security for ports of member countries of the Organization; and (4) organizing and conducting annual courses planned under the Inter-American Port Security Training Program.

Caribbean Customs Law Enforcement Council

Established in the 1970s, the Council has 35 signatory countries including the United States and other members of the Organization of American States, as well as several European countries with interests in the Caribbean Basin. The mission of the Council is to assist member administrations to fulfill their mandates to (1) collect and protect revenue, (2) prevent and interdict illicit drugs and other prohibited and restricted goods, and (3) facilitate legitimate trade and international travel through the use of modern business systems. Its efforts focus on improving communications, information and intelligence systems, training and development of customs officers, customs reform and modernization, and promoting continued cooperation between member customs administrations and other enforcement agencies.

International Maritime Organization Resolution on Commercial Maritime Drug Smuggling

The International Maritime Organization (a component of the United Nations) Resolution A.872(20), which was adopted by the Organization in November 1997, establishes guidelines for the prevention of drug smuggling on ships engaged in international maritime commerce. The resolution, is titled *Guidelines for the Prevention and Suppression of the Smuggling of Drugs, Psychotropic Substances and Precursor Chemicals on Ships Engaged in International Maritime Traffic.* Although written from the vessel operator's viewpoint, the resolution is considered a precedent-setting document containing language that could serve as a foundation for a companion resolution on port and cargo security from the landside perspective.

Key International Organizations on Seaport Security Issues

Achieving solutions requires a multilateral partnership among governments, the international commercial maritime industry and trade community, and constituents of the world economy. A cooperative international approach depends on the commitment of all states to sustain their participation in multilateral organizations. Promoting cooperation against transnational organized crime committed against the maritime industry is more effectively organized through such organizations. They include, for example, the International Maritime Organization, United

Nations, International Criminal Police Organization (INTERPOL), International Association of Airport and Seaport Police, International Council of Cruise Lines, American Association of Port Authorities, International Chamber of Commerce, Baltic and International Maritime Council, and World Customs Organization.

The International Maritime Organization, an active and well-respected organization, was created as a convention at an international conference in Geneva in 1948, which recognized that shipping is perhaps the most international of the world's industries. The International Maritime Organization fosters international cooperation on maritime issues. Recently the organization has been addressing issues specifically related to terrorism and crime, so it might provide a forum for some of the issues raised in this report.

The Commission visited the International Maritime Organization headquarters in London to discuss the status of international security guidelines, recommendations, or standards and the process for initiating international port security guidelines or standards. This visit confirmed that, except for cruise ship and terminal security guidelines, and guidelines for governments and ship owners in combating piracy, there are no international port security guidelines. The Organization has passed a resolution establishing guidelines for the prevention of drug smuggling on ships engaged in international commerce. The Organization's representatives indicated that if the United States or another nation were interested in proposing the development of international port security guidelines, the International Maritime Organization would be the proper international forum.

INTERPOL, established in 1914, ensures and promotes widespread mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries and in the spirit of "Universal Declaration of Human Rights." INTERPOL is designed as a communications organization and does not maintain a force of international police officers or agents. Instead, it serves as a conduit for a cooperative exchange of criminal information to help detect and combat international crime. INTERPOL provides a forum for discussion, working group meetings, and symposia to enable police from the member countries to focus on specific areas of criminal activity affecting their countries.

Two organizations that offer monetary solutions and support to nations are the International Monetary Fund and the World Bank. The International Monetary Fund promotes monetary cooperation through a permanent forum for consultation and collaboration on international monetary issues. The World Bank provides development assistance to client nations. The World Bank's purpose is to help people help themselves and their environment that includes forging partnerships in the public and private sectors. Both of these organizations are lending institutions that expect repayment of their monetary assistance. In developing counties, it is frequently the case that governments lose substantial revenues because they lack adequate control of their borders, including seaports, and therefore fail to collect legitimate import duties and taxes associated with foreign trade. The International Monetary Fund and the World Bank may attach conditions to their loans requiring countries to shore up their port infrastructure, reduce corruption, and improve border security in order to stem this loss of revenue. These organizations have significant leverage over the behavior of foreign governments and could make use of such loan conditions to promote the objectives of combating crime and enhancing security in foreign seaports.

The World Customs Organization, established originally as the Customs Cooperation Council, is an intergovernmental body composed of 150 customs administrations.

The group has been working for decades to foster cooperation and harmonization among customs operations throughout the world. One very significant achievement was the harmonization of the global tariff codes, which number more than 20,000—a project so complex that it required more than 20 years to complete. The organization in June 1999 adopted a model customs code that would harmonize all customs procedures globally.

The International Chamber of Commerce has as its members the major businesses throughout the world that are interested in international trade issues. The group has committees that are concerned with shipping and customs issues.

International Best Practices

To gain an appreciation for how U.S. seaports compare with international seaports, the Commission visited two large seaports overseas and identified their best practices. The Commission selected the ports of Felixstowe, United Kingdom, and Rotterdam, the Netherlands, for visits because of their significant infrastructure and their advanced use of technology. The Commission attempted to identify the areas that make the ports successful.

The Commission also met with representatives of the British government concerned with seaport security: the Department of the Environment, Transport, and the Regions, the Security Service, and the Home Office Coordinator for Ports Policing. Of particular note was the existence of a national-level committee that deals with port security issues.

Felixstowe showcased a robust in-house security operation. The port police have full police powers but are employees of the port. This relationship, while efficient and a model of professionalized seaport security, creates a conflict of interest from the perspective of what amounts to a private law enforcement agency. The perimeter security (fence), closed-circuit TV system, and access control procedures at the port were excellent.

Rotterdam highlighted several important security practices, including a state-of-the art container X-ray facility. The most important practice was its methods for certification of private security officers. In the Netherlands, as noted earlier in this report, all private security officers must be graduates of government-approved security courses and must pass national exams. This certification process is conducted at every level of private security, including management, and it enhances the professional reputation of private security officers as well as increasing their competence. Rotterdam emphasizes seaport security by designating a Harbor Police Division within its police department.

Findings and Recommendation

Finding 8.a. The security of foreign seaports has a direct impact on the security of U.S. seaports. Shipping and cargo originating in or transiting foreign ports provide an avenue for the introduction of transnational threats to the United States.

Finding 8.b. Maritime cargo is increasingly vulnerable to criminal exploitation during transaction points throughout the landside shipping cycle.

Finding 8.c. Increased involvement overseas by U.S. law enforcement agencies engaged cooperatively with their foreign counterparts is essential to proactive policing of international cargo crime and improving the results of law enforcement efforts.

Finding 8.d. Three key international organizations could serve as a forum to promote international cooperation and standards in the areas addressed in this report:

the International Maritime Organization, the World Customs Organization, and the International Chamber of Commerce.

Finding 8.e. Several U.S. agencies provide international port security training to our trading partners.

Finding 8.f. The port of Rotterdam, in the Netherlands, with its state-of-the-art container X-ray facility, national certification of private security officers, and specialized harbor police division, could provide adoptable best practices and serve as a model port.

Recommendation 19. Work internationally to strengthen global seaport security by:

- Continuing implementation of the President's International Crime Control Strategy and other related strategies.
- Promoting, through federal agency initiatives and diplomatic channels, the development by cognizant international organizations of appropriate international guidelines for addressing seaport crime and security issues. These organizations include the International Maritime Organization, INTERPOL, the Organization of American States, the World Bank, the International Monetary Fund, and other relevant intergovernmental and non-governmental organizations.
- Increasing cooperation and information-sharing with foreign law enforcement and customs agencies.
- Expanding training in seaport security for less-developed countries that are trading partners. Such training should be targeted toward countries where there are serious problems and/or special law enforcement concerns. Topics should include anti-corruption, export control, and handling of transit goods.

Chapter 9: The State of Security in U.S. Seaports

Introduction

Seaports are critical components of the nation's borders that serve as gateways for the movement of international commerce. Port security measures are aimed at minimizing the exploitation or disruption of maritime trade and the underlying infrastructure and processes that support it. Seaports face threats from criminals and terrorists. A variety of criminal enterprises target seaports and their land and waterside approaches to exploit these intermodal transfer points for the purpose of perpetrating a range of economic crimes including trade fraud, cargo theft, and smuggling. Terrorists and rogue states intent on attacking U.S. interests could target the critical infrastructure that includes the transportation and information networks that support U.S. economic power and the peacetime transportation capabilities depended upon to support deployment of military forces for national security contingencies. Seaport vulnerabilities may stem from inadequate crime prevention and security measures, as well as the challenge of monitoring the vast and rapidly increasing volume of cargo, persons, and vessels passing through U.S. ports. To what degree are U.S. seaports at risk?

Key Findings

In assessing crime and security at U.S. seaports, the Commission found substantial evidence indicating that the problem of serious crime in seaports is significant. Drug smuggling is the most prevalent and most readily documented criminal activity, but smuggling of contraband, stolen goods, prohibited or restricted merchandise and illegal aliens, trade fraud, unlawful exportation of controlled commodities and munitions, and environmental crimes are also occurring in seaports. In addition, while instances of seaport criminal activity directly linked to terrorism are rare, much of the criminal activity regularly occurring in seaports (particularly contraband and alien smuggling) is by nature susceptible to exploitation by terrorists in conducting their operations. Moreover, while the threat of terrorism against seaports themselves is currently regarded as low, critical seaport infrastructure is vulnerable to direct attack.

The Commission was unable, however, to assess the full extent of serious crime in seaports, or to conclusively establish relevant trends. There are currently no reporting systems in place that provide an accurate and comprehensive picture of serious crime in seaports. Federal agency databases do not adequately collect and report crime incidents by seaports, nor are there adequate state or local government databases to draw upon. Moreover, there are strong indications that a high percentage of crime in seaports goes unreported and often undetected.

Most crimes in seaports are violations of federal law, typically directly related to the import or export of goods or contraband. Federal agencies are responsible for regulating the import and export of cargo, the movement of vessels, and the entry and departure of persons, as well as for countering contraband and alien smuggling through seaports. Most state and local law enforcement agencies support the overall anti-smuggling effort, but focus primarily

on property and violent crimes committed in seaport areas.

Seaport security is a complex issue that encompasses a broad array of threats and vulnerabilities, and involves numerous key actors including federal, state, and local law enforcement and inspection agencies; port authorities; private sector businesses; and organized labor and other port employees. In addressing seaport security, the Commission focused on three primary areas:

- The routine border control activities of certain federal agencies, most notably Customs, the Coast Guard, and the Immigration and Naturalization Service, in seeking to ensure that the flow of cargo, vessels and persons through seaports complies with all applicable U.S. criminal and civil laws.
- The nature and extent of physical security at seaport facilities.
- The ongoing efforts of certain federal agencies, most notably the Coast Guard, the Federal Bureau of Investigation and the Department of Defense, in seeking to ensure that critical seaport infrastructure is safeguarded from major terrorist attack or other catastrophic accident.

In the first area, the Commission found that each of the responsible federal agencies has inspection and enforcement programs that target seaports in a comprehensive and generally effective manner given the volume of maritime traffic and the level of agency resources available for this task. That said, there were many indications that seaport border control programs can and should be improved. Current resource allocations are a primary determinant of the level of federal border enforcement efforts, and agencies too often find themselves in a reactive mode in addressing the full range of seaport crime. The significant and high-profile drug smuggling threat typically commands most of the available resources, with other contraband smuggling, commercial fraud and export crime receiving much less attention.

While trade volumes have grown tremendously and are expected to double every 10 years, for the most part agency staffing at seaports has not kept pace, limiting the ability of the federal government to detect, respond to, and prevent criminal activity in seaports. Although there have been many significant investigative and law enforcement accomplishments, and there are additional efficiencies yet to be gleaned (primarily through increased use of technology and enhanced information sharing), the relevant federal enforcement agencies believe that more personnel and other resources would help address seaport crime and security issues. However, they recognize that increases must be considered in the context of the overall budget development process.

As reflected in the Commission's recommendations, potential improvements in the border control realm may be realized through broader and more effective use of technology; changes to the existing statutory and regulatory structure governing the flow of cargo, vessels, and persons through seaports; and better coordination and partnership among agencies at all levels of government and with the private sector.

In terms of both physical security and safeguarding seaport infrastructure, field surveys revealed that security measures (including control of access to marine terminals and other facilities) vary from port to port, but generally range from fair to poor. In several cases, security is good. No widely accepted security standards or guidelines exist for seaports and their facilities. Responsibility for seaport security is fragmented, with coordination and cooperation among all levels of government and the private sector generally not optimal. The limited intelligence and other information available on seaport security issues is not consistently shared with all of those who should have that information. Few

threat or vulnerability assessments of seaports and their facilities are conducted.

The Commission found that substantial work has been done at the national level in preparing strategies and establishing formal structures for coordinating government efforts to address seaport security, either directly or indirectly. This work relates primarily to preventing drug and other contraband smuggling; promoting marine transportation safety; protecting critical infrastructure; and combating terrorism. Many of these initiatives, however, have not yet reached the level of individual seaports. Too many seaport authorities remain largely unaware of ongoing criminal activity, the potential for terrorism, and the way in which appropriate security measures can deter crime and decrease vulnerabilities. The Commission believes that many seaport entities have not given adequate attention to these security issues and that more effective interagency and public/private sector efforts are needed in this regard.

Seaports are critical border control points that afford law enforcement unique opportunities to employ warrantless searches of cargo and persons to intercept contraband and other goods being transported illegally into the country. The effectiveness of this border control function has crime and national security implications for all parts of the United States, not only the seaports. A key facet of seaport security must be to protect the integrity of the border control function, and thereby to help control crime and promote national security generally.

The Commission recognizes that one standard security regime will not be appropriate for all seaports. Seaports across the United States vary significantly in size as well as the nature and scale of operations. The major seaports are multi-billion dollar enterprises, while many others receive only a few vessels a year. Some seaports handle large volumes of bulk hazardous cargoes such as petroleum or liquefied natural gas, while others move low-risk bulk commodities such as grain, or specialize in intermodal freight containers. In certain ports, unique geography or the proximity of specific high-risk facilities heightens the vulnerability to potential terrorist acts or catastrophic accidents. The recommendations advanced by the Commission reflect the widely varying circumstances affecting seaports and the necessity to tailor security improvements accordingly.

The major findings upon which the Commission based its recommendations may be summarized as follows:

- Internal conspiracies are one of the most serious crime problems, particularly with respect to drug smuggling. Trafficking organizations routinely use transportation industry employees to facilitate their smuggling operations at seaports by controlling or monitoring the movement of the legitimate cargo in which drug shipments are concealed.
- Cargo theft is the crime that is most important to the private sector business entities that operate in seaports. While the majority of cargo thefts occur when shipments are in transit away from seaports, the seaports provide central locations where organized crime groups can locate and easily target a wide variety of high value goods. The absence of a nationwide system for collecting and reporting cargo theft data has hampered both assessment of this problem and the development of appropriate solutions.
- The threat of terrorism directed at U.S. seaports is low, but should not be discounted. Although seaports represent an important component of the nation's transportation infrastructure, there is no indication that they are currently being targeted by terrorists.
- The vulnerability of U.S. seaports to terrorist attack is high, and the potential consequences of such attack are significant from a national security standpoint.

Ports provide a venue for the introduction of a host of transnational threats into the nation's infrastructure. Further, the nexus of transportation modes as well as the concentration of passengers, high-value cargoes, and hazardous materials make seaports potential targets for terrorist attacks.

- Inadequate physical security at seaport facilities undercuts law enforcement efforts. A fundamental cause of this condition is the absence of uniform security standards and operating guidelines. The access of persons and, more importantly, commercial and privately owned vehicles to vessels, cargo receipt and delivery operations, and passenger processing areas should be controlled in order to more effectively deter and prevent crime.
- Unlike airports, seaports do not have separate and restricted areas where vessels, cargo, and passengers arriving from foreign locations are processed. Areas in which federal inspection (Customs, Immigration, and Agriculture) takes place are not well controlled, undercutting the effectiveness of these inspections and at times posing a security risk to federal inspection personnel.
- Private security personnel are a vital component of overall seaport security and cargo control. However, competencies in critical tasks and service performance vary widely among security companies, highlighting the potential for private security to compromise the federal interest in seaports.
- The U.S. trade system is vulnerable to cargo diversion and commercial smuggling. The process of clearing goods is complex and highly dependent on both electronic systems and timely inputs from commercial sources, both of which need significant improvement. Vessel manifest information, import and export, is often inadequate for import risk assessment and export cargo control. As one example of current shortfalls, the shipper's export document—a key source of information used by law enforcement officials to identify illegal exports—is usually filed up to four days after the actual sailing of the vessel carrying the goods. This delayed filing effectively removes any real control from the administration of export regulations. Another example is that the Customs "in-bond" system for the movement of foreign or restricted merchandise through the United States is susceptible to abuse in ways that deprive the government of revenue, compromise international trade agreements, and at times endanger American consumers.
- The federal agency automated systems for tracking cargo and vessels are not easily accessible from waterfront facilities or are at remote container examination stations. Lack of ready access undercuts agency efficiencies, enforcement activities, and commercial compliance initiatives.
- Existing federal statutes, regulations, and sentencing guidelines do not provide sufficient sanctions for civil and criminal violations. Civil penalties for failures to comply with cargo documentation requirements are commercially inconsequential when compared to cargo values and shipping fees. While criminal sentences potentially available for drug trafficking provide significant deterrents, other criminal activity (e.g., cargo theft) does not entail the same sentencing risk, yet it is often more lucrative.
- Joint task forces of federal, state, and local law enforcement have proven to be successful in combating crime in certain seaports, and cooperation among law enforcement agencies could be further improved through increased joint planning efforts and cross training. However, resource constraints often hampered agencies' participation in task forces and

other interagency partnerships among federal, state, and local law enforcement. Ongoing cooperation between federal agencies and the private sector (e.g., the Customs Carrier Initiative) is impressive and should be expanded where appropriate.

- Adequate equipment and security-enhancing technology is not available at most seaports. Few seaport facilities employ best practices and available technology to enhance cargo security. Equipment (such as cameras, carbon dioxide detectors, and vessel tracking devices) that would assist law enforcement personnel in accomplishing their missions is not always available to field personnel. The level of inspection and detection technology available at seaports has generally not kept pace with that available at other border locations, such as airports and the Southwest land border. Acquisition costs for such new equipment and technology could be kept to a minimum by co-locating federal agencies at seaports and initiating a joint planning process for technology.
- Information about the movement of vessels, people, and cargo within seaports is not integrated, nor is it always readily available to government and private sector security organizations responsible for detecting, intercepting, and preventing criminal activity (including terrorism). In addition, there is inadequate actionable intelligence on seaport crime made available to law enforcement agencies. This process of sharing and disseminating information should be monitored by the local port security committee to ensure that information of security awareness, and intelligence information on criminal activity, port vulnerabilities, and terrorist threats is shared among government agencies and with the private sector where appropriate.
- The security of foreign seaports has a direct effect on the security of U.S. seaports. Shipping and cargo originating in or transiting foreign ports provide an avenue for the introduction of transnational threats to the United States. Maritime cargo is highly vulnerable to criminal exploitation at transaction points throughout the landside shipping cycle. Increased involvement overseas by U.S. law enforcement agencies engaged cooperatively with their foreign counterparts is essential to improved international enforcement efforts.

Optimizing Resources

The Commission did not undertake a resource allocation study. However, many statements were volunteered in the seaports surveyed indicating that there are clear perceptions within agencies and the private sector that changes in trade patterns and federal agency resources have not kept pace. Customs has recently developed a resource allocation model. A number of other agencies have also developed and employed such planning devices. All agencies involved in seaport security need to be certain that they have evaluated their resource allocation and budget development in accordance with increased trade volumes, enhanced use of information management and screening technology, and other relevant projections affecting federal agency staffing levels. They should consider as well the appropriate mix of federal, state, and local assets needed to adequately address crime and security within seaports.

The Commission's recommendations, detailed at the end of each chapter and highlighted in the Executive Summary, have significant crime control and other national security implications. Substantial resources will be required to implement many of them. These resources may be reprogrammed from within a department's base funding or new resources in addition to base funding. The Commission urges that the findings and recommendations

of this report be accorded prominence for agency policy, program, budget, and regulatory purposes. To the extent that the recommendations have resource implications, the Commission recognizes that they must be weighed against other priorities in the context of the overall budget process.

Summary

As barriers to trade and travel across international boundaries are reduced and volumes of international cargo and passengers grow, opportunities for criminals to exploit the commercial transportation system grow as well. In the absence of positive action to identify threats and reduce vulnerabilities, U.S. seaports will remain at risk from criminals trafficking in drugs, illegal migrants, weapons, and other contraband, and engaging in fraud, theft, and terrorism.

Although much of the investment in security infrastructure and protection of port facilities is the responsibility of state and local governments or private sector security managers, a lead role for coordinating seaport anti-smuggling and counterterrorism activities lies with the federal government. Presidential Decision Directive 63 clearly states that the federal government will take the lead in bringing together private sector interests in protecting critical infrastructure, including seaports.

While physical, procedural, and personnel security enhancements at seaports will require added investments in equipment, personnel, and training, such measures may significantly reduce the vulnerability of port infrastructure, vessels, waterfront facilities, persons, and cargo to terrorist attack or other criminal activity. Increasing the difficulty of exploiting the legitimate commercial cargo system for smuggling of drugs, illegal migrants, stolen vehicles, and other contraband can also greatly limit opportunities for the introduction of weapons of mass destruction through seaports. These factors, coupled with the increasing dependence upon commercial seaports for the deployment of U.S. military forces abroad, have national security implications far beyond reductions in smuggling and cargo theft. A robust program aimed at improving port security undertaken by federal inspection and law enforcement agencies, state and local governments, port authorities, and the private sector can generate measurable reductions in seaport vulnerability that will enhance national security, reduce crime, and improve the economic well-being of the United States.

Finding 20. Assessing the adequacy of personnel resources contributing to seaport security is complicated by a combination of many factors. Any such assessment would need to address the following points, among others: (a) all relevant personnel, including criminal investigators, inspectors, analysts and support staff; (b) the interdependency of the federal agency personnel who comprise the "federal team" at seaports; (c) possible application of current and planned approaches to personnel issues associated with air and land ports of entry; and (d) the optimal overall mix of federal/state/local/private sector personnel and other assets needed to provide an appropriate level of security, including border control, at seaports.

Recommendation 20. Consider initiation, through the new proposed national-level security subcommittee, of a comprehensive, interagency study to analyze the impact of current projections related to seaport crime, trade volumes, technology, and other key factors on future personnel requirements for federal agencies having border control responsibilities at seaports.

Appendix A: Executive Memorandum Establishing the Commission

THE WHITE HOUSE

WASHINGTON

April 27, 1999

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF AGRICULTURE
THE SECRETARY OF COMMERCE
THE SECRETARY OF LABOR
THE SECRETARY OF HEALTH AND HUMAN SERVICES
THE SECRETARY OF TRANSPORTATION
ADMINISTRATOR OF THE ENVIRONMENTAL PROTECTION AGENCY
DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET
UNITED STATES TRADE REPRESENTATIVE
DIRECTOR OF NATIONAL DRUG CONTROL POLICY
CHIEF OF STAFF TO THE PRESIDENT
DIRECTOR OF CENTRAL INTELLIGENCE
ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF

SUBJECT: Establishment of the Interagency Commission on Crime and Security in U.S. Seaports

United States seaports are an integral part of our Nation's commerce. Too often, however, they tend to be a major locus of crime, including drug trafficking, cargo theft, and smuggling of contraband and aliens. Moreover, the criminal conspiracies often associated with these crimes can pose threats to the people and critical infrastructures of seaport cities.

Many government agencies at the Federal, State, and local level are addressing this significant problem, at times in partnership with the private sector. I have determined that the Nation needs a comprehensive review of the nature and extent of seaport crime and the overall state of security in seaports, as well as the ways in which governments at all levels are responding to this problem.

Therefore, I hereby direct as follows:

1. The Secretary of the Treasury, the Attorney General and the Secretary of Transportation, in cooperation with other heads of executive departments and agencies as appropriate, shall establish the Interagency Commission on Crime and Security in U.S. Seaports (hereinafter, the Commission).

2. The Commission shall be comprised of not more than 25 members and shall be co-chaired by 3 Federal officials, one of whom shall be appointed by the Secretary of the Treasury, one of whom shall be appointed by the Attorney General, and one of whom shall be appointed by the Secretary of Transportation.

3. The Commission members shall include senior officials of: the Departments of State, the Treasury, Defense, Justice, Agriculture, Commerce, Labor, Health and Human Services, and Transportation; the Environmental Protection Agency, the Office of Management and Budget, the Office of National Drug Control Policy, the Central Intelligence Agency, the National Security Council, and the Joint Chiefs of Staff. All members of the Commission shall be full-time Federal employees.

4. The Commission shall undertake a comprehensive study of the nature and extent of the problem of crime in our seaports, as well as the ways in which governments at all levels are responding. The study shall address all serious crime relating to the maritime context, including but not limited to drug trafficking, cargo theft, and the smuggling of contraband and aliens. Moreover, the study shall carefully examine the role of internal conspiracies often associated with such crime in seaports, including the potential threats posed by terrorists and others to the people and critical infrastructures of seaport cities.

5. In the course of its work, the Commission shall seek input from, and take full account of, the expertise and views of the many different State and local government agencies with relevant responsibilities, as well as the involved private sector interests.

6. The Commission shall complete its work within 1 year of the date of its establishment. On or before that date, the Commission shall submit a report to the Secretary of the Treasury, the Attorney General, and the Secretary of Transportation, including the following:

- 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;

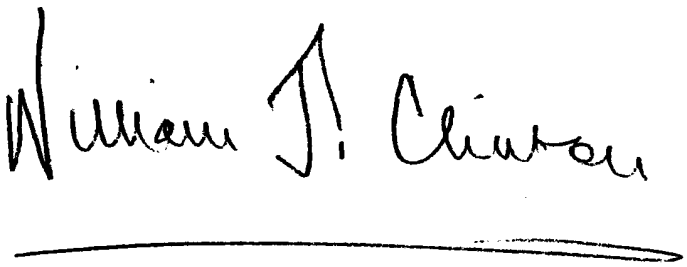
- An assessment of the nature and effectiveness of the ongoing coordination among the Federal, State, and local government agencies; and

- Recommendations for improving the response of Federal, State, and local governments to the problem of seaports crime.

7. Within 3 months of the submission of the Commission's report, the Secretary of the Treasury, the Attorney General, and the Secretary of Transportation shall forward the report, together with their joint recommendations, to the Chief of Staff to the President for final review and appropriate action.

8. The Secretary of the Treasury shall appoint an Executive Director who will oversee the support staff and a working group to be established to further the work of the Commission. The Executive Director shall report directly to the Co-Chairs of the Commission.

9. With the exception of the personnel costs (including the salaries and any necessary travel expenses) of the members of the Commission and the working group, which shall remain the responsibility of their parent agency, the Department of the Treasury shall fund the Commission, including all costs for support staff, office space, and logistics.



Appendix B: Methodology

Scope

There are 361 public seaports in the United States. They have a broad range of characteristics. Many seaports are small and have limited commerce; only 144 have over a million tons of cargo. In the larger seaports, the activities can stretch along a coast for many miles, including public roads within their geographic boundaries. The facilities used to support arriving and departing cargo are sometimes miles from the coast. The inland seaports accept mostly bulk products such as grain, petroleum, coal, or steel. The seaports that accept international cargo have a higher risk of international crimes such as drug and alien smuggling. The top 50 ports in the United States account for about 90 percent of all cargo tonnage. In terms of container shipments, 25 U.S. seaports account for 98 percent of the cargo. Cruise ships visiting foreign destinations embark from 16 ports.

Generally, seaport geographic boundaries are defined. However, criminal activity associated with the cargo that comes into the seaport does not always occur on the seaport grounds, or it is not detected until after the cargo leaves the port. For example, crime may be suspected and federal agents may engage in a surveillance that may not be culminated until many days or weeks later and hundreds of miles away. Frequently, cargo arrives in U.S. ports and the importer files in-bond documents to move cargo to another city, maybe thousands of miles away. Technically the cargo is still under federal supervision until importers file their final entry in another location and it is released by Customs. Finally, in those seaports where security is improved, the industry has found that cargo thefts occur after the cargo leaves the seaport grounds. There is a wide variation in examining crimes that occur within the strict confines of a seaport and crimes that include those related to the cargo that is imported or exported. And there is a lot of middle ground. For this effort, the Commission addressed security and crime within the port boundaries and international cargo remaining under federal supervision. In addition, the Commission reviewed existing information on cargo crime in the seaport's metropolitan area.

Far from being self-contained entities, seaports should be viewed as part of an intermodal and international trade corridor. Ensuring cargo security and preventing and reducing crime at U.S. seaports really starts when the cargo is loaded by manufacturers or when it is loaded onto the vessels at the foreign ports. Starting when the vessels reach U.S. seaports leaves out critical points in the process where crimes can be initiated. Although the Commission's primary focus is to review security and crime in U.S. seaports, the Commission addressed, to a limited extent, vessels being boarded and loaded in foreign countries and en route to their destination on the high seas.

In addressing criminal activity in U.S. seaports, the issue of what crimes should the Commission study arises. The Presidential Memorandum directing the establishment of the Commission uses terms such as "seaport crime," "crime in our seaports," and "all serious crime with a nexus to the maritime context." Criminal activity involving U.S. seaports can generally be viewed in three broad categories: (1) criminal

activity committed by smugglers, thieves, or other criminal groups whose criminal activity is aided and abetted by corrupt individuals employed within the transportation industry (commonly referred to as internal conspiracies), (2) criminal activity that exploits legitimate international trade or otherwise utilizes the transportation industry to facilitate crime, and (3) crimes that comprise the Part I and Part II offenses in the Uniform Crime Reporting Program. The list below shows the types of crimes that the Commission included in its efforts:

- Terrorism.
- Internal conspiracies involving all substantive crime.
- Smuggling: strategic/sensitive items (weapons of mass destruction, drugs, munitions, currency, precursor chemicals, etc.).
- Smuggling: general (child pornography; art/artifacts, endangered species, etc.).
- Alien smuggling; stowaways.
- Cargo theft (metropolitan area, federal supervision).
- Cargo control (false manifesting, diversion, substitution, etc.).
- Trade crime (intellectual property rights, dumping, child labor, etc.).
- Extortion, racketeering, money laundering, tax evasion, bribery, corruption, and other serious crimes.
- Health and safety (tainted foodstuff, pharmaceutical drugs, chlorofluorocarbons, pesticides, etc.).
- Environmental crimes (dumping oil, hazardous waste, toxic substances, etc.).
- Unlawful export of strategic/sensitive items (weapons of mass destruction, ballistic delivery systems, critical technology, military equipment, munitions, currency, etc.).
- Unlawful exports of general items (stolen vehicles, property and securities, U.S. trade secrets, economic espionage, etc.).

In addressing security (which we view as the preventative side) at U.S. seaports, the following categories have been identified as core issues: physical security and access control; cargo security; passenger and crew security; and military mobilization security. Effective physical security and access control in seaports is fundamental to deterring and preventing potential threats to seaport operations, cargo shipments for smuggling or theft, or other cargo crimes. Securing entry points, open storage areas, and warehouses throughout the seaport, controlling the movements of trucks transporting cargo through the port, and searching containers, warehouses, and ships at berth or in the harbor are important requirements. Identification procedures for arriving workers, and deterring and preventing internal conspiracies, are also becoming increasingly important. Unconstrained by jurisdictional constraints or national borders, criminal organizations are exploiting weak security in seaports and their intermodal connections to commit a wide range of cargo crimes. Levels of containerized cargo volumes are forecasted to increase significantly, which will create more opportunities for crime while lowering the statistical risk of detection and interdiction.

The large number of U.S. citizens sailing on international cruises provides an attractive target to terrorists seeking to cause mass casualties. Approximately 80 percent of cruise line passengers are U.S. citizens and 20 percent are aliens. Approximately 92 percent of crewmembers are aliens. Cruise ships pose a special risk from a security perspective. The worldwide cruise ship fleet will carry nearly 10 million cruise passengers this year. Cruise ship terminals must be secure to prevent unauthorized people from gaining access to the area. Coast Guard regulations exist that specify minimum security standards to which cruise ship lines must

adhere to in order to adequately protect passengers from terrorist attacks. These regulations apply only to large cruise ships on international voyages. In contrast, ships with domestic voyages (that do not dock at a foreign port) such as sightseeing, gambling, and fishing vessels, as well as commuter and car ferries, are not covered under the regulations. Security programs in these sectors are voluntary. Costs associated with enhancing security often prevent these business sectors from pursuing a solid security program.

If U.S. troops and equipment are needed in other parts of the world, they are generally deployed through U.S. commercial seaports. In the event of a contingency, U.S. military and logistical support for overseas operations must now extend greater distances over shorter time lines in order to reach the military theater of operation. Consequently, U.S. seaports have become critical choke points of future military mobilizations. The security of our commercial ports during times of military mobilization ensures that such movements are not disrupted and is, therefore, essential to the national defense.

Ports Under Study by the Commission

The Commission reviewed the listing of 361 commercial seaports to determine which seaports we should study in depth. With only 50 seaports representing 90 percent of all cargo by tons, 25 ports representing 98 percent of the container traffic, and 16 ports representing 98 percent of all international cruise ship passengers, we decided to confine the scope of on-site surveys to 12 seaports.

The Commission performed on-site surveys at 12 seaports, with the primary focus on those seaports that receive international cargo. The seaports were selected based on their size and level of criminal activity. They are:

Charleston	New Orleans
Detroit	New York/New Jersey
Gulfport	Philadelphia
Los Angeles	Port Everglades
Long Beach	San Juan
Miami	Tacoma

The Commission collected data at each location it surveyed. It toured ocean and land facilities and reviewed security practices. It examined port and terminal facilities, warehouses, and federal inspection stations, along with other port facilities. Many seaport officials were interviewed, including the following:

- Port authorities and terminal operators.
- State and local law enforcement officials.
- Other state and local government officials.
- Ocean, truck, and rail carriers.
- Warehouse operators.
- Foreign trade zone operators.
- Freight forwarders and customs brokers.
- Importers and exporters.
- Private security groups.
- Labor unions.
- Officials of federal agencies including the Bureau of Alcohol, Tobacco, and Firearms, the Animal Plant Health Inspection Service, the Commerce Department, the Coast Guard, the Consumer Product Safety Commission, the Customs Service, the Department of Defense, the Drug Enforcement Administration, the Environmental Protection Agency, the Federal Bureau of Investigations, U.S. Attorney's Offices, the Food and Drug Administration, the Internal Revenue Service, the Food Safety Inspection Service, the Immigration and Naturalization Service, and the Maritime Administration.

The following national and international organizations provided input to the Commission:

- American Association of Exporters and Importers.
- American Association of Port Authorities.
- American Institute of Marine Underwriters.
- American Trucking Associations.
- American Waterways Operators.
- International Council of Cruise Lines.
- International Longshore and Warehouse Union.
- International Longshoreman's Association.
- Maritime Security Council.
- National Cargo Security Council.
- American Association of Waterfront Employers.
- American Institute of Marine Underwriters.
- National Customs Brokers and Forwarders Association.
- Technology Asset Protection Association.

The Commission also published a notice in the Federal Register to give the private sector and public an opportunity to comment in public sessions. These sessions were set in Hampton Roads, Virginia; Houston, Texas; and San Francisco, California. A Web site was established on the Internet to provide information about the study to the general public and to solicit comments from those who could not contact the Commission in person. Commission members and the staff also attended conferences of relevant national organizations and solicited comments from many private organizations.

Work Plan

In order to accomplish its work, the Commission developed a comprehensive methodology. The methodology included the following sections:

I. Describe the specific mission, authorities, and responsibilities of federal agencies and identify the roles played in security by federal, state, and local governments as well as the private sector.

II. Analyze the nature and extent of serious crime with a nexus to the maritime context.

III. Assess the readiness of seaports to respond to terrorist threats.

IV. Evaluate the state of security at U.S. seaports.

V. Assess the nature and effectiveness of ongoing coordination among federal, state, and local government agencies.

VI. Solicit input from the private sector and other interests.

Each section and the work efforts undertaken for the Commission's efforts are described in more detail below.

Section I: Describe the Specific Missions, Authorities, and Responsibilities of Federal Agencies and Identify the Roles Played by Federal, State, and Local Governments as well as the Private Sector

Seaports are complex entities with hundreds of different organizations conducting business, often with tens of thousands of employees working for them. The Maritime Administration estimates that the port industry, nationwide, results in more than 13 million jobs, about $500 million in personal income, $1.5 trillion in business sales, about $750 billion in GNP and about $200 billion in taxes. Public seaports are generally owned and operated by local governments through a Port Authority; however, large portions of seaport real estate are often leased to the private sector with the local government operating as a landlord. In addition, many privately owned and operated terminals exist within seaports, independent of the local Port Authority. Businesses operating in the seaport include terminal operators, ocean carriers, and trucking companies as well as warehousemen, freight forwarders, brokers, and food servicing companies.

Crime that occurs in the seaport may be investigated by a number of agencies. State or local law enforcement officers combat much crime at seaports, but the federal government also has a role. The Customs Service, Immigration, and other inspection agencies such as the Food and Drug Administration and the Agriculture Department are also involved to ensure that cargo and passengers arriving from foreign countries comply with U.S. laws and regulations. Smuggling merchandise such as illicit drugs, weapons of mass destruction, conventional weapons, child pornography, and counterfeit merchandise also attract federal agency interest. Seaports also serve as a mechanism for undocumented or illegal aliens to enter the United States. Terrorist threats and environmental crime involve even more agencies.

Collecting Federal Agency Information

To describe the authorities, missions, and responsibilities in each federal agency, the Commission contacted each to obtain legislation, regulations, executive orders, and other sources that provide information about agency authorities regarding crime and security at seaports. We also surveyed agencies to determine which agencies have grant authority. The Commission identified the specific organizational components that deal with crime and security at seaports and their mission-related objectives.

Agency Programs on Crime and Security at U.S. Seaports

Several agencies have developed programs that deal with crime and security at U.S., as well as foreign seaports. For example, the Customs Service has a Carrier Initiative Program in which the agency works with carriers to improve their security in U.S. and foreign ports, as well as the Americas Counter Smuggling Initiative and the Business Anti-Smuggling Coalition program, which are designed to assist foreign businesses and governments in deterring and preventing narcotics from being smuggled via legitimate businesses, and to assist importers, exporters, and port authorities in deterring smuggling, respectively. Although these programs were initially designed to prevent drug smuggling, the improvements in security assist the businesses for other areas as well. The Maritime Administration, in conjunction with the Organization of American States, conducts a maritime security training program for ports in foreign countries. The Commission also briefly looked at some of the key federal control functions in the seaport and in the approaches to seaports, focusing on the areas of maritime security, law enforcement, cargo inspection and control, and passenger/crew inspection and control.

Section II: Analyze the Nature and Extent of Serious Crime with a Nexus to the Maritime Context

One of the key objectives of the Commission was to conduct an analysis of the nature and extent of serious crime in U.S. seaports. In order to do this, the Commission had to collect as much information as possible from federal, state and local law enforcement agencies relating to seaport crime. This was difficult because most federal, state, and local law enforcement agencies typically do not collect and report crime data by seaports.

For example, the Bureau of Justice Statistics, a component of the Office of Justice Programs in the Department of Justice, is the primary source for criminal justice statistics, but none of its programs collect and report crime data by seaport. In addition, the Uniform Crime Reporting Program and the National Incident-Based Reporting System are nationwide crime data collection and reporting systems administered by the Federal Bureau of Investigation, but these programs also do not collect and report crime data by seaport.

The Commission's crime data collection effort occurred in two main areas. First, the Commission collected data from all relevant federal agencies for fiscal years 1996 through 1998. Crime data were collected from the Customs Service, the Drug Enforcement Administration, the Federal Bureau of Investigation, the Department of Commerce, the Immigration and Naturalization Service, the Coast Guard, the Bureau of Alcohol, Tobacco, and Firearms, the Internal Revenue Service, the Department of Agriculture, the Environmental Protection Agency, and the Food and Drug Administration. The type of crime data collected consisted of known offenses, arrests, seizures, recoveries, and information on internal conspiracies (industry employees).

Second, the Commission conducted on-site studies at the 12 seaports surveyed, where crime data were collected from appropriate state and local law enforcement agencies from 1996 through 1998 and where interviews and meetings were held with appropriate federal, state, and local law enforcement officials to discuss crime problems at seaports. During the on-site study, the team conducted the following activities:

- Met with relevant federal, state, or local law enforcement officers knowledgeable in seaport crime to discuss their estimates and views, and how they are responding to seaport crime.
- Met with appropriate U.S. Attorney representatives who are knowledgeable in the prosecution of seaport crime to determine what prosecution efforts are underway relative to seaport crime and their ideas for improvement.
- Met with federal, state, and local law enforcement agencies knowledgeable in seaport crime to discuss their recommendations to improve anti-crime efforts at seaports.
- Met with relevant federal, state, and law enforcement officers knowledgeable in seaport crime to discuss intelligence initiatives, as well as the crime threat facing their seaports and their recommendations for improvement.
- Met with relevant federal, state, and local law enforcement officers knowledgeable in seaport crime to discuss technology issues and their recommendations for technology improvements.

Section III: Assess the Readiness of Seaports to Respond to Terrorist Threats

The Commission reviewed the issues related to addressing possible terrorist acts at seaports. In addressing the issue of possible terrorist attacks at seaports, the Commission examined if seaports are vulnerable to terrorist incidents, and how security within seaports could contribute to a possible terrorist incident. The Commission also examined the ways in which government agencies are responding to the threat of possible terrorist incidents at seaports and provide recommendations for reducing vulnerabilities and improving the response of federal, state, and local governments to these threats.

Many government agencies have found that by establishing partnerships with the maritime industry and trade organizations that provide incentives for industry to participate in programs, they can enlist the trade's support in law enforcement initiatives. Because of the effect that a terrorist activity could have at a seaport and industry's interest in preventing or thwarting this type of activity it was anticipated that carriers, port authorities, and other affected organizations would want to work closely with the Commission on this issue.

The Commission also focused on ways to develop and disseminate actionable intelligence to law enforcement agencies (including state and local) regarding: the identification of illegal trafficking in weapons of mass destruction, illicit financial transactions involving terrorists, and the identification of possible terrorist targets at seaports. The Commission also reviewed ways that the federal agencies are providing the private sector with information. Information could permit the private sector to target suspicious shipments and individuals who could be using a U.S. seaport to transport terrorist-related materials, or who could be choosing a target within the seaport area such as a cargo vessel, port facility, cruise ship, bridge, or oil storage tanks to attack.

The Commission addressed how well ports throughout the country have prepared for terrorist threats and evaluate what the Federal government is doing to assist them. The Commission decided to:

- Work with the Federal Bureau of Investigation, Department of Defense, Navy, Department of Transportation, Central Intelligence Agency, National Security Council, and other agencies to collect available information on terrorist threats to U.S. seaports and maritime commerce, in general.
- Identify if and how information about terrorism and terrorist threats is disseminated to the port authorities and carriers for them to prepare for threats.
- Review with port authorities and terminal operators their knowledge of terrorist threats and determine what steps they have taken to prepare.
- Review with carriers, for both cargo and passengers vessels, their knowledge of terrorist threats and determine what steps they have taken to prepare.
- Solicit suggestions for improvements.

Section IV: Evaluate the State of Security at U.S. Seaports

To evaluate the state of security at seaports, the Commission needed a set of standards or criteria to use as a benchmark. Unfortunately, there has not been comprehensive federal rulemaking on security at seaports as there has been at airports. There are also no generally accepted international or industry standards for all components of seaport security. Therefore, the Commission needed to develop a set of standards to use for the purpose of this evaluation.

Security Criteria

In developing standards for seaport security to be used by the Commission, many sources were evaluated including federal regulations, government handbooks, and guidelines of private sector groups that have devoted substantial efforts to improving security. A set of criteria was compiled which provide a basis for key elements of seaport security. The criteria, compiled from commercial industry port security standards and federal agency guidelines, represent reasonable and defensible minimum levels of performance. The Commission developed a two-tier approach. The first tier was a minimum set of standards that have been accepted as good practice by the various business and government groups that have studied these issues. A second tier was designed enhanced security measures that have been either proposed or are in effect in some seaports. The seaports were evaluated using the first set of criteria. However, the Commission collected information at the seaports on the enhanced security measures to determine if the level of commitment to security is higher in some areas and to see how they are working. The criteria developed by the Commission for evaluating security pertain to four functional components as follows:

- *Physical security and access control* refers to perimeter security, for both port and facility boundaries and internal restricted areas, and may include fences, gates, lighting, alarm systems, and security patrols. It should also include identification and access restrictions for employees, casual labor, visitors, vehicles, and vessels.
- *Cargo security* includes screening of shipments for contraband (drugs, currency, stolen vehicles, prohibited exports, etc.), as well as implementing measures to prevent theft of cargo from marine terminals or en route to or from the seaport, or smuggling of contraband concealed in containers along with legitimate cargo shipments.
- *Passenger and crew security* includes protecting vessel passengers and crew from terrorist attack, preventing unauthorized entry into the seaports of illegal migrants or stowaways on commercial vessels, and preventing smuggling of drugs or other contraband by vessel crewmembers.
- *Security for military mobilization* includes measures to ensure physical, operational, and information security for overseas deployment of U.S. military equipment, ammunition, and supplies through commercial seaports in order to prevent sabotage, espionage, and terrorist attack.

A complete set of criteria is included at the end of this appendix.

Field Work and Survey Techniques

To further its study and analysis, the Commission conducted on-site surveys at 12 U.S. seaports, including some Strategic Seaports, where the Commission conducted security surveys of entities within the ports (vessel operations, pier and terminal operations, warehouses, trucking terminals, and rail facilities). The surveys were conducted by using entity-specific surveys developed and designed to assess the security of passenger, cargo, and military operations within the port, and the overall physical security of the port. The Commission also reviewed existing plans and threat assessments and the dissemination of intelligence within seaports. The Commission surveyed two foreign ports and compared the security at these foreign facilities to that at the 12 U.S. seaports surveyed.

Section V: Assess the Nature and Effectiveness of Ongoing Coordination Among Federal, State, and Local Government Agencies

Assessing the effectiveness of coordination is a complex task because coordination is difficult to measure and quantify. There are also no widely accepted standards on effective coordination. After much consideration, the Commission decided to conduct the assessment in this section by interviewing the various entities and asking a series of questions about how they work together. The Commission also saw some difference in the way coordination might occur in the area of criminal activity versus security and prevention. Although law enforcement authorities do pursue criminal activity both proactively and reactively, a significant amount of time and effort is spent reacting to criminal activity. The purpose of security is to deter and prevent crime and unauthorized intrusions. Most frequently, the officials who pursue the crimes are not the same as those who pursue security.

The Commission identified current U.S. interagency and intergovernmental initiatives and activities that address crime and security in the seaport environment. Once these initiatives and activities were identified, the Commission examined whether the efforts are sufficient to ensure safe and crime-free seaports.

Because there are no set measures that quantify whether cooperation is at an acceptable level, the Commission identified several areas for review, including communication and liaison, training, intelligence sharing and results, operational coordination, and accomplishments.

The Commission is also aware that businesses and other entities involved in seaport operations are critical to improving security and combating crime. Many of the security procedures are implemented by the private sector such as ocean carriers, truckers, and warehousemen. Employees who work at the seaports are also a critical link. Businessmen and employees sometimes are willing to serve as informants to law enforcement agencies. The Commission also reviewed efforts the federal, state, and local agencies have ongoing to work with this important sector of the seaport community.

Section VI: Solicit Input from the Private Sector and Other Interests

The issues involving port security within U.S. seaports affect many different entities in a variety of ways. For example, carriers, importers/exporters, and freight forwarders often suffer when security practices in a port are lax because their operations become vulnerable to smugglers and thieves. Also, an individual port's reputation may suffer because if it fails to correct deficient security practices, it may be perceived as fostering environments that allow thieves and smugglers to exist. The lack of security can therefore relate to increased business costs for the individual trade entities that use a port, or in the loss of business by ports.

There are trade associations in the private sector whose goals are to reduce cargo theft and pilferage, such as the National Cargo Security Council. There are associations with interests in reducing their vulnerability to drug and alien smuggling and maritime terrorism, such as the Maritime Security Council, the International Council of Cruise Lines, and the American Association of Port Authorities. These associations represent carriers, importers/exporters, insurance companies, port authorities, and others who have an interest in reducing the vulnerability of their members. Many of these entities and associa-

tions are currently involved in partnerships with government agencies in order to identify and address security-related issues and to reduce their overall vulnerabilities. The experience and knowledge that these entities and organizations could offer to the Commission had the potential to make the Commission's evaluations more effective and accurate, and to ensure that the Commission's recommendations are realistic and can be effectively implemented.

It was anticipated that labor groups would also be a significant stakeholder regarding the issue of security within U.S. seaports. Labor organizations perform the lading and unlading of cargo at many U.S. seaports, and other organizations perform tasks related to the movement of goods within ports. These and other groups have an interest in security-related issues in ports.

Identifying and soliciting input from stakeholders was accomplished by:

- Interviewing the headquarters of federal agencies and congressional offices to determine the organizations and groups they normally consult with on these issues.
- Contacting local federal agency offices to determine the organizations and groups they consult with on these issues.
- Meeting with private sector and labor groups during the on-site surveys.
- Publishing a notice in the *Federal Register* regarding the establishment of the Commission and soliciting input from the stakeholders.
- Creating a Web site to disseminate information to stakeholders about the establishment of the Commission and to outline its objectives.
- Attending and speaking to the attendees of industry conferences and law enforcement conferences.
- Speaking with all of those from the private sector or state and local governments who wished to make a presentation to the Commission.

Port Security Criteria

The following details the criteria used to evaluate seaport security and review possible enhancements as described in Chapter 5. The sources used to compile this information are included in the footnotes.

Physical Security and Access Control[1]

Perimeter Fence Line

- Fence line should be intact, taut, well secured to upright supports anchored into the ground, topped with barbed wire on outward facing angle irons, and stand at least eight feet in height.
- Reinforcement of the fence line with a barrier (e.g., ditch or berm) should be used to enclose wheeled operations involving containers on chassis or trucks with consolidated cargoes overnight, to render certain parts of the fence line physically impassable for a trailer.
- Alarms should be installed to complement the security of a reinforced fence line to form a system capable of monitoring many alarm zones from a central control room manned by terminal security personnel.

---

[1] *Standards for Marine Cargo Security,* Security Committee, American Association of Port Authorities, 1980; *Measures To Prevent Unlawful Acts Against Passengers and Crews On Board Ships* {Assembly Resolution A.584(14)}, International Maritime Organization (IMO), 1986; Physical Security for Cargo and Passenger Terminals, *Maritime Security Manual,* Seaports and Harbors Subcommittee, Standing Committee on Transportation Security, American Society for Industrial Security, 1990; *Terminal Security,* TT Club; 1997 [TT Club is a European-based specialist insurer of transport operators equipment and liabilities operating in 80 countries]; *Port Security: Security Force Management,* authored by Port Authority of New York/New Jersey Police and private sector seaport security consultants; published by U.S. Department of Transportation, 1998.

Parking

- Parking areas shall be situated outside of fenced operational areas or a substantial distance from cargo handling and storage areas and buildings, and passenger embarkation areas.
- Employees exiting to the parking area from a cargo or passenger facility shall be required to pass through a controlled area under the supervision of security personnel.
- Employees visiting their motor vehicle during work shifts should be required to notify management or security personnel.
- Control of access to employee parking areas should be supervised, and shall be restricted by a permit system with records maintained that include matching personnel with permit number and motor vehicle identification. Temporary permits will be issued to vendors and visitors for parking in designated controlled areas.

Access Points

- Gates in disuse should be permanently sealed or removed.
- Gates considered indispensable and in daily use should be secured by two sets of padlocks and case-hardened steel chains, or deadlocking bolt or an equivalent device, which does not require use of a chain.
- Gates should be equipped with a recording system to document inspection stops by security personnel during routine patrols.
- Separate gates shall be constructed for the use of personnel and vehicular traffic, which will include personnel screening point.
- Gate alarms should be installed and monitored from a central point (e.g., main guard house).
- Gatehouses at all vehicle entrances and exits shall be manned during business hours by operators of facilities handling a substantial volume of high value cargo, should be situated so that exiting vehicles may be halted and examined on terminal property, and be equipped with telephones or other communications devices.
- Closed circuit television systems should be used for control of the interior and perimeter of the terminal and record entry and exit through the main gate, and the images stored for designated periods.
- Operational information obtained by terminals during the entry stage should be made available to the security department for its purposes to, for example, ensure and verify that a particular container was released to a specific driver.

Lighting

- Controlled adequate lighting shall be provided to enable clear illumination for all facility areas, including perimeter fence lines, entrances, exits, and gatehouses, and sufficient to assure proper visibility of approaching persons and vehicles.
- Seaport authority should ensure that all areas of the terminal are illuminated to at least the level of twilight, even when there is no activity. While in port, the ship deck and hull should be illuminated in periods of darkness and restricted visibility, but not so as to interfere with the required navigation lights and safe navigation.

Buildings

- In areas adjacent to warehouses, sheds, and passenger terminals a buffer zone of at least 10 feet should be created around the entire building and be enforced at all times.

- Remove containers obstructing the view of building entrances by police and security guards.
- All exterior doors and windows should be equipped with properly installed locks or locking devices, and incorporated with detection or alarm systems.
- Area alarm systems should be installed to secure computer rooms and office spaces where confidential documents are stored.
- Key control system should be implemented with a formal policy governing which personnel have right of access to specified areas, and include a master ledger maintained recording the legitimate holder of each copy of each key, and issuance for which shall be controlled by management or security personnel.
- Locks, locking devices, and key control systems will be inspected regularly, and malfunctioning equipment repaired or replaced.

Standard Operating Procedures

- Port authority or terminal operator shall provide current security manual incorporating standard operating procedures, standards of conduct, and a definitive statement of what the management expects of the security force.
- The security manual should be fully documented, complete, and accurate, and be consistently adhered to.
- Security director should formulate written operating procedures for security-related matters, including bomb threats and alert levels, and should collaborate with relevant government and law enforcement agencies to develop an emergency response plan.
- Adequate and reliable communications should be provided to enable contact between elements of the terminal security force and from the security force to local law enforcement.
- An employee identification card system shall be employed by terminals handling a substantial volume of cargo or passengers to identify personnel authorized to enter cargo, passenger, and document processing areas.
- Display of employee identification card, visible at all times, shall be required of each employee.
- Supervisory personnel should be present during lunch and breaks if taken in the work area.
- Truck drivers, vendors, and other visitors should not be permitted in the general offices of any terminal other than as required to conduct their business, and only authorized personnel should be permitted in warehouses.
- Computer security formal guidelines should be in place for each marine terminal.
- Computerized information access must be password controlled, and should be restricted on a need-to-know basis, which would include dissemination of information no sooner than required to complete transactions involving, for example, shipping agents.

Security Force Management

- Security director should establish minimum hiring standards, and ensure their compliance.
- Training is imperative for in-house or contracted security force personnel, all of whom must receive adequate pre-work classroom training and certification by a qualified professional that includes completion of basic security topics, and should have at least 16 hours of on-the-job training.
- Security director's written job specifications should include the task of maintaining and validating the published information in the security manual, should be an assessment element in the manager's formal performance review.

- Security personnel should frequently patrol terminals to ensure that gates, fence line, and buildings are secure.
- Security personnel should be required to complete a work sheet during each shift, recording the duties performed by them and at the times of occurrence.

Enhanced Measures for Physical Security and Access Control

- *All individuals employed in the seaport who have access to restricted or secure areas have been subject to background and criminal record checks.*
- *In addition to port facility employees, photo ID badges are displayed by vessel crewmembers, other carrier employees, vendors, longshoremen, passengers and visitors to prevent unauthorized access to restricted areas.*
- *Intrusion Detection Systems including video monitoring, remote sensors and alarms, and computerized recording instrumentation are employed to facilitate real-time evaluation and response and subsequent investigation and analysis.*

Cargo Security[2]

Delivery of Cargo

- Gate passes must be issued to truckers and other carriers to control and identify those authorized to pick up cargo.
- The company name of carriers must be clearly shown on all equipment.
- Cargo should only be released to the carrier specified in the delivery order unless a release authorizing delivery to another carrier is presented and verified.
- Personnel processing delivery orders should verify the identity of the trucker and trucking company before releasing the shipment.
- Access to areas where documentation is processed must be limited to only authorized personnel and shipping documents need to be safeguarded from theft.
- Seal numbers on containers should be verified against documents, and seals should be checked for integrity.
- The insides of conveyances should be checked for stolen merchandise.
- Drivers should sign for shipments legibly and in ink.

Reception of Cargo

- Drivers entering facilities with deliveries must obtain gate passes.
- Drivers should show identification and the company name of carriers must be clearly shown on all equipment.
- Delivery documents (such as bills of lading) should be closely scrutinized, seal numbers on containers should be verified against documents, and seals should be checked for integrity.
- Cargo shipments should be verified upon receipt.

Security of Cargo during Lading and Unlading from Vessels and Railcars

- Cargo should be moved directly from railcars or vessels directly to storage facilities, and directly from storage facilities to railcars and vessels.
- Seals should be checked on all containerized shipments prior to arrival/departure/transfer.
- Empty containers should be opened, examined, and resealed, and stored door to door in facilities.

[2] Treasury Decision 72-56, dated February 4, 1972; *Sea Carrier Security Manual,* Customs Publication No 546, April, 1989; *Terminal Security,* published by the TT Club; *Cargo Security and Loss Control,* published by the National Cargo Security Council, 1998; *Security Recommendations and Standards for Cargo Security,* compiled by the International Association of Airport and Seaport Police, 1984.

Storage of Loose Cargo

- Cargo stored in open areas, and palletized or stacked cargo stored in warehouse facilities must be properly stacked and placed within, away from, and parallel to fences and walls, to ensure unimpeded views for security personnel.

Documentation Review and Control

- Bills of lading for cargo and containers should be checked for accuracy prior to acceptance.
- Cargo on documentation should be adequately described, and the weights and piece counts indicated on documentation.
- Cargo documentation should be closely guarded to avoid documentation fraud.

Cargo Control, Inventories, and Cargo Reconciliation

- Facility operators must maintain, and continuously update an accurate list (paper or electronic) of all cargo in facilities and a location chart of all cargo, and containers in their facilities.
- Import cargo, export cargo, and domestic cargo should be segregated.
- Delivery and receiving operations should be segregated.
- Overages and shortages should be reported immediately.

High Value Merchandise

- High value commodities must be stored in cribs or security cages designed to resist forcible entry from all sides, and separate logs and procedures for the release and receipt of these commodities must be maintained.
- High value merchandise in mounted containers must be placed in a secure holding area where it can be observed by management or security personnel at all times and separate logs and procedures for the release and receipt of these containers must be maintained.
- High value cargo in containers should also be placed on the upper tiers of container stacks in order to limit their accessibility, and the containers should also be stacked so that the doors of each container abut each other.

Seals and Sealing Practices

- Seals must be inspected whenever a sealed containerized shipment enters or leaves a facility. If the seals are not intact, or there is evidence of tampering or the seals are not correct, security needs to be notified and the cargo in the container needs to be tallied.
- Unsealed containerized shipments need to be sealed at the point of entry to the facility and the seal number needs to be noted on shipping documents.
- Seals must be stored in a secure place, access to seals must be restricted, and a log noting the distribution of seals must be kept.
- Seals must also be checked and their numbers, date, time, and place of examination recorded at each of the following times: arrival at/leaving the terminal gate, during stacking; relocation within the terminal; loading/discharge from a vessel; whenever the container doors are opened.

Equipment Control

- Access and keys to equipment such as yard mule tugmasters, trucks, or high loaders should be strictly controlled.
- Equipment should be kept in a secure and specified area when not in use.

Personnel Security

- Perspective employees should be required to provide background information about previous employment history, criminal records, and drug use.
- All prospective employees should be fingerprinted as part of the application process and criminal history records

should be performed on all perspective employees (to the extent permitted by law).

- Employers should have "drug awareness" and "security education" programs in effect for all employees.
- Employees must wear distinctive identification cards or badges that act as authorization for accessing restricted areas.

Audit Trails, Correcting Vulnerabilities, and Reviewing Procedures

- Procedures must be in place that will permit investigators when reviewing documentation to determine how and when any cargo or containers were removed from an operator's custody in an unauthorized manner.
- When an operator's system is compromised, and cargo or containers are removed from an operator's custody in an unauthorized manner, procedures must be in place to identify the deficient procedures/practices and corrective action must be taken to ensure a similar incident does not occur.
- Managers must review procedures periodically to ensure new threats and procedural vulnerabilities are identified as they arise.

Enhanced Measures for Cargo Security

- *Seaports where foreign cargo arrives should have a separate Federal Inspection Station. Access to these areas is limited only to those that have previously received approval to enter the area.*
- *Closed Circuit Television system should be used to record activities during lading and unlading procedures, and within cargo processing and trucking facilities.*
- *Port Authorities, terminal operators, warehouse operators, and trucking companies have installed automated access control systems in order to monitor access to restricted areas.*
- *Port Authorities, or terminal operators, employ non-intrusive technology (such as X-ray, or gamma ray systems) to identify contraband and/or verify cargo shipments.*
- *Trucking company uses an automated system such as Global Positioning Systems or cellular) to track trucks and shipments.*
- *Firms have developed and implement "Integrated Security Concepts" into their operations to deter and prevent internal conspiracies from occurring.*

Security of Passengers and Crew[3]

- The introduction of prohibited weapons, incendiaries, or explosives aboard passenger vessels, on persons, within personal articles or baggage, or in stowed baggage, cargo, or stores should be prevented or deterred.
- A high level of gangway security should be maintained by passenger vessels throughout a voyage. These security measures should include some form of biometric identifier (such as a photograph), to prevent the unauthorized boarding and re-boarding of persons after port calls.
- Timely, accurate, and complete passenger and crew arrival and departure manifest information should be submitted by carriers to the Immigration and Naturalization Service.

[3] International Civil Aviation Organization (ICAO) Convention on International Civil Aviation, Annex 17: International Standards and Recommended Practices; U.S. Code of Federal Regulations, Title 14, Part 107 (Airport Security), Part 108 (Airplane Operator Security), Part 109 (Indirect Air Carrier Security); United Kingdom—Aviation and Maritime Security Act of 1990; International Maritime Organization (IMO)—Maritime Security Committee Circular 443: Measures to Prevent Unlawful Acts Against Passengers and Crews on Board Ships; International Maritime and Port Security Act (46 USC app. 1801)—Title IX of the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (PL 99-399); U.S. Code of Federal Regulations, Title 33, Part 120 (Security of Passenger Vessels), Part 128 (Security of Passenger Terminals).

- All members of a passenger vessel's crew should be adequately trained to perform their security-related duties.
- Physical and operational security measures should be coordinated between passenger terminals and passenger vessels whenever a vessel is moored at the terminal.

Enhanced Measures for Passenger and Crew Security

- *Seaports where international passengers arrive should have a separate Federal Inspection Station. Access to these areas is limited only to those that have previously received approval to enter the area.*
- *Visitors/Passengers gain access to a terminal facility through a designated screening point that should include a metal detector and X-ray system.*
- *The use of automated access control or magnetic stripe cards is utilized over the use of keys to enter terminal facilities.*
- *The Advance Passenger Information System is utilized by carriers and is submitted in a timely fashion to the Immigration and Naturalization Service and Customs so that law enforcement checks can be performed prior to a vessel's arrival in the United States.*

Military Mobilization Security

- The local Port Readiness Committee must actively meet. All applicable federal, state, local, and commercial entities must be included in its membership.
- The Port Readiness Committee must have a written and current memorandum of understanding.
- A Port Readiness Exercise must have been conducted within the last two years.

Enhanced Measures for Military Mobilization Security

- *Any "lessons learned"/problems, as outlined in the latest Port Readiness Exercise Final Report, must be resolved or in the process of being actively resolved.*
- *The local Coast Guard Captain of the Port must address security for military mobilization in their planning documents.*
- *If a Department of Defense vulnerability assessment was done on this port, the vulnerabilities, if any, must have been adequately addressed by the Port Readiness Committee.*

Appendix C: Related Initiatives About Seaport Security

One of the first tasks the Seaport Commission undertook was to survey what had already been done by the federal sector that pertained directly to the tasks set forth in the Presidential Memorandum. The Commission's study and this report are related to these efforts in a number of ways. It is important to understand each of the other efforts and their relationship to the focus of this report. The Commissioners overseeing this report decided that the work of the Seaport Commission would be consistent with current policy and that it would not duplicate or re-research areas that other study groups had already covered. A few of the more significant efforts of other groups are summarized below.

A National Security Strategy for a New Century, December 1999

This strategy, released by the White House in December 1999, contains three core objectives: to enhance America's security, to bolster America's economic prosperity, and to promote democracy and human rights abroad. The strategy addresses the following topics:

- Threats to U.S. interests such as regional or state-centered threats, transnational threats, spread of dangerous technologies, failed states, foreign intelligence collection, and environmental and health threats.
- Shaping the international environment (diplomacy, international assistance, arms control and nonproliferation initiatives, military activities, international law enforcement cooperation, and environmental and health initiatives).
- Responding to threats and crises (transnational threats, terrorism, drug trafficking, and other international crime).
- Emerging threats at home (national missile defense, countering foreign intelligence collection, preparedness against weapons of mass destruction, critical infrastructure protection, and national security emergency preparedness).
- Small-scale contingencies (humanitarian aid, peace operations, enforcing embargoes and no-fly zones, evacuating U.S. citizens, and reinforcing allies).
- Major theater warfare.
- Promoting prosperity by strengthening financial coordination, promoting an open trading system and enhancing American competitiveness through technological advantage, export advocacy, enhanced export control, providing for energy security, and promoting sustainable development.
- Promoting democracy and human rights abroad.
- Integrating regional approaches.

The *National Security Strategy* is relevant to seaports in three major ways. First, seaports, because of their multimodal nature, are a nexus where a number of elements of the nation's critical infrastructure meet. The portal effect of a seaport as an entry point to the United States serves to heighten its importance to U.S. national security interests. Further, the seaport is vulnerable to a host of transnational threats including terrorism, drug and alien smuggling, and fraudulent activity. Clearly, the

nation's seaports are vitally important elements of the nation's critical infrastructure.

Second, seaports are a vital link for energy. Almost half of the cargo tonnage that enters U.S. seaports is petroleum or petroleum products.

Finally, with the end of the Cold War and the resultant military draw-down and withdrawal from foreign bases, some of our domestic commercial ports have taken on increased importance as endpoints of the Sea Lines of Communication and as Seaports of Embarkation for military forces being deployed for contingencies worldwide. The importance of our commercial seaports as venues for deployment of military forces underscores the vital importance of U.S. seaports to the national interest.

International Crime Control Strategy, May 1998

This strategy, released by the White House in May 1998, recognizes that international criminals engage in a wide range of illegal activities, including drug trafficking, terrorism, alien and contraband smuggling, fraud, extortion, money laundering, bribery, economic espionage, intellectual property theft, and counterfeiting. The strategy sets these eight goals:

- Extend the first line of defense beyond U.S. borders.
- Protect U.S. borders by attacking smugglers and smuggling-related crimes.
- Deny safe haven to international criminals.
- Counter international financial crime.
- Prevent criminal exploitation of international trade.
- Respond to emerging international crime threats.
- Foster international cooperation and the rule of law—for instance, by establishing international standards.
- Optimize the full range of U.S. efforts, including coordination, partnership with the private sector, and measurement of progress.

Most of the crimes that are described in the strategy occur at seaports, and because agencies such as Customs, the Border Patrol in the Immigration and Naturalization Service, and the Coast Guard have authority to conduct border searches on the water and on the border, seaports are a convenient and cost-effective location to pursue such crimes. Fostering international cooperation and establishing international standards are also relevant to this effort.

National Drug Control Strategy, 1999

This strategy, published by the Office of National Drug Policy Control in 1999, sets five goals:

- Educate and enable America's youth to reject illegal drugs as well as alcohol and tobacco.
- Increase the safety of American citizens by substantially reducing drug-related crime and violence.
- Reduce the health and social costs to the public of illegal drug use.
- Shield America's air, land, and sea frontiers from the drug threat.
- Break foreign and domestic drug sources of supply.

Countering drug trafficking has consistently been the role of Customs, the Coast Guard, and the Drug Enforcement Administration, both in the port and on the water. Again, the special border search authority makes the seaport and the high seas productive and fruitful locations to combat drug trafficking. In addition, it is more cost-effective to interdict drugs before the supplies are cut or distributed among numerous individuals and entities.

International Organized Crime and Cargo Theft, December 1999

According to the report prepared by the Central Intelligence Agency, international organized crime groups could be responsible for as much as half of the estimated $30-50 billion in cargo stolen worldwide each year. Key findings include:

- Russian and other syndicates have infiltrated key transportation hubs—including air and seaports in Asia and Europe—and appear to tap information-sharing networks to identify lucrative cargo.
- Syndicates look for cargo with high resale value and pre-sell some of these to unscrupulous buyers. The groups are highly mobile and able to elude law enforcement.
- Crime groups typically target regions experiencing economic or social turmoil to take advantage of burgeoning black markets for other goods.
- Law enforcement will be hard pressed to disrupt cargo theft along key transit routes because prosecution rates are poor and regulations governing stolen cargo are not standardized.
- Syndicates also will most likely target commercial shipping systems and Internet Web sites.

This effort is relevant to the Commission's effort in that it demonstrates that cargo theft is a global concern. Cargo theft, or piracy, can occur on the high seas, near the port, or on the port grounds. Cargo theft represents an area where international cooperation could serve U.S. efforts as well as those in other countries.

Report of the White House Commission on Aviation Safety and Security, February 1997

President Clinton created the Commission on Aviation Safety and Security to look at the changing security threat and determine how to address it; to examine changes in the aviation industry and how the government should adapt to them; and to look at technological changes coming to air traffic control and what should be done to take advantage of them for security purposes. The report was issued in February 1997, and the recommendations relevant to security are these:

- Consider aviation to be a national security issue, and provide substantive federal funding for capital improvements.
- Assess the possible use of chemical and biological weapons as tools of terrorism.
- Establish consortiums of federal, state, and local governments and the private sector at all commercial airports to implement enhancements to aviation safety and security.
- Secure access to airport-controlled areas, and ensure the physical security of aircraft.
- Establish federally mandated standards for security enhancements.
- Establish a security system that will provide a high level of protection for all aviation information systems.
- Conduct airport vulnerability assessments and develop action plans.
- Aggressively test existing security systems.
- Require criminal background checks and Federal Bureau of Investigation fingerprint checks for all screeners and employees with access to secure areas.
- Work with industry to develop a national program to increase the professionalism of the aviation security workforce, including screening personnel. Certify screening companies and improve screener performance.
- Significantly expand the use of bomb-sniffing dogs.
- Use the Customs Service to enhance security.

- Give properly cleared airline and airport security personnel access to classified information they need to know.
- Improve passenger manifests.
- Implement a comprehensive plan to address the threat of explosives and other objects in cargo, and work with industry to develop new initiatives.
- Significantly increase the number of FBI agents assigned to counterterrorism investigations, to improve intelligence and crisis response.
- Deploy existing technology.
- Establish a joint government-industry research and development program.
- Create a central clearinghouse within the government to provide information on explosives crime.
- Submit a proposed resolution, through the U.S. representative, that the International Civil Aviation Organization begin a program to verify and improve compliance with international safety standards.
- Provide antiterrorism assistance in the form of airport security training to countries where there are airports served by airlines flying to the United States.
- Provide regular, comprehensive explosive detection training programs for foreign, federal, state, and local law enforcement, as well as Federal Aviation Administration and airline personnel.

It was important for the Commission to review these recommendations and consider their application to the seaport environment. This effort did not address crime at airports; it aimed to examine vulnerabilities, especially related to terrorist activities. In some senses our study is broader; however, the airport effort did place heavy emphasis on safety issues such as the air traffic controller system.

Critical Foundations—Protecting America's Infrastructure, October 1997

The report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations—Protecting America's Infrastructure,* was released in October 1997. That Commission looked at elements of the critical infrastructure—energy, banking and finance, transportation, vital human services, and telecommunications—and found that they must be viewed in a new context in the Information Age. Its findings were the following:

- Information sharing is the most immediate need.
- Responsibility for protecting the infrastructure is shared among owners and operators (the private sector) and government.
- Infrastructure protection requires integrated capabilities of diverse federal agencies and special means for coordinating the federal response to ensure that these capabilities are melded together effectively.
- The challenge is one of adapting to a changing culture.
- The federal government has important roles in the new infrastructure protection alliance with industry and state and local governments.
- The existing legal framework is imperfectly attuned to dealing with cyber threats.
- The current level of research and development is not adequate to support infrastructure protection.

With regard to the transportation sector, the Commission recommended that the Department of Transportation take the lead and:

- Establish a central office for coordinating intermodal infrastructure assurance for examining terrorism issues, includ-

ing prevention, mitigation, contingency response, recovery, and coordinating with other federal agencies on those issues.

- Develop joint government/industry response and recovery plans with the private sector.
- Establish an improved information dissemination and sharing process.
- Test the effectiveness of the dissemination process and of established security procedures.
- Work more closely with industry on research and development and education.
- Request funding and positions to manage these emerging issues.
- Provide government security clearances to industry.
- Develop security and infrastructure assurance education programs.
- Perform crosscutting research on assurance issues.
- "Red Team" and test critical Department of Transportation systems and industry systems on a cooperative, selective basis.
- Sponsor and conduct industry symposiums and workshops.

Seaports are part of the nation's critical infrastructure. These recommendations are relevant and needed to be considered as part of the Commission's review of seaports.

Presidential Decision Directive 40: U.S. Port Security Program, September 1995

National security interests require that measures be taken to control the access of foreign-flag vessels to U.S. ports, internal waters, and territorial seas. Presidential control is exercised through the National Security Council. The NSC directed the Commandant of the Coast Guard to implement a program in coordination with the Departments of State, Defense, Treasury, and Justice and the federal intelligence community. The Coast Guard Captain of the Port exercises authority under the Magnuson Act of 1950 and regulations 33 CFR 6 to enforce provisions including controlling vessel movements and denying entry to U.S. ports as necessary.

Worldwide Maritime Challenges

The report entitled *Worldwide Maritime Challenges* was jointly prepared by the Department of State, the Coast Guard, the Immigration and Naturalization Service, the Customs Service, and the Department of the Navy. The report identified the following 11 categories of challenges to maritime security:

- *Multinationals-multiflags:* The borderless finances of multinational corporations have blurred the focus on who controls ship and cargo movements. For protection, support, interdiction, and monitoring, it is increasingly difficult to know precisely who is being affected and who may be called for assistance.
- *Smuggling:* Illicit trade at sea includes smuggling of narcotics and illegal aliens, transfer of unauthorized technology, or seaborne transfer of other illegal or untaxed cargoes.
- *Sealift support:* Although airlift can provide short-term support, sealift is the key to sustaining operations for whatever time is required to complete the effort.
- *Sanction violations:* Arms or trade sanctions levied by the United States, the United Nations, or other international organizations are often violated or circumvented by deceptive trade practices, false shipping and cargo documentation, stealth, and other means.

- *Mass migration:* Economic or political refugees traveling via the sea can quickly tax the resources of U.S. maritime forces and humanitarian organizations.
- *Arms trafficking:* Monitoring arms flow is an essential element in predicting future instability and in assessing forces with which the United States and its allies may have to contend.
- *Crime and violence:* Terrorism, piracy, and other crimes at sea are injurious to commerce, stability, and freedom of the sea.
- *Weapons of mass destruction:* The legal and illegal trade in weapons of mass destruction, components, and precursors can alter the balance of power and endanger a population and the environment.
- *Trade access:* The sea is a common highway; no nation should deny access to the United States or its allies.
- *Environmental protection:* The maritime environment is increasingly vulnerable, and the concern goes far beyond the beaches.
- *Maritime food supply:* The sea is a source of food supply that should be protected.

Threats and Challenges to Maritime Security 2020, March 1999

The report entitled *Threats and Challenges to Maritime Security 2020* was published in March 1999 by the Office of Naval Intelligence and the Coast Guard Intelligence Coordination Center. It was intended to be an information tool for policymakers, strategic planners, integrated systems analysts, and force structure planners. The report identified the following significant changes affecting the maritime threat by 2020:

- Legal maritime trade will triple.
- Nonstate actors, such as environmental groups and multinational corporations, will have more influence.
- Organized crime will increase in influence and scope.
- Adversaries of the United States will be more likely to engage in asymmetric warfare such as terrorism, sabotage, information operations, and chemical or biological attacks.
- The capabilities of space-based ocean monitoring systems will increase.
- Exploitation of nonliving marine resources (such as oil and minerals) will increase.

In addition, the report cited the following issues of today that will continue as pressing issues through 2020:

- Worldwide demand for fish will increase.
- Drug trafficking will continue to plague the United States.
- International migration will continue to increase.
- Degradation of the marine environment will continue.

An Assessment of the U.S. Marine Transportation System, A Report to Congress, September 1999

In November 1998, Congress mandated that the Coast Guard, the Maritime Administration, and other interested agencies "assess the adequacy of the nation's marine transportation system (including ports, waterways, harbor approach channels, their intermodal connections) to operate in a safe, efficient, secure, and environmentally sound manner." The agencies' effort was essentially an assessment of where the maritime industry was going during the next 20 years and what steps were necessary to prepare for its future. The focus areas included coordination, competitiveness, infrastructure,

environmental, national security, and safety.

The interests in national security were to keep the flow of traffic moving and to safeguard the nation's waterways, ports, facilities, vessels, individuals, and property in the vicinity of the port from accidental or intentional damage, destruction, loss, or injury. The Marine Transportation System (MTS) initiative is closely linked to the Interagency Seaport Commission via seaport security issues. Of particular importance to the Seaport Commission's security assessment of U.S seaports is the MTS Report's "Security" strategic area discussion. Within this "Security" strategic area, the MTS report highlighted five action areas: improving security awareness, improving transparency, ensuring qualified operators, forging stronger public/private partnerships, and strengthening international cooperation.

Many of the recommendations contained within these five MTS security action areas defer to the assessment of seaport security being done by the Seaport Commission. Specifically, the MTS security recommendations below were extensively studied by the Seaport Commission. Following each MTS security recommendation below is a brief synopsis of the Seaport Commission's position and, where appropriate, a link to a specific Seaport Commission recommendation.

- *"Improve Security Awareness":* Support the Interagency Commission on Crime and Security in U.S. Seaports to heighten national awareness of the need for collective action and to develop a coordinated interagency approach to Marine Transportation System ports and waterways security.

  Comment: As extensively discussed in Chapters 5 and 6, the Seaport Commission strongly supports the development of a coordinated interagency approach to improving security awareness in our nation's seaports. Specifically, we recommend using the Marine Transportation System National Port Readiness Network and local Port Readiness Committees to focus attention on enhancing seaport security through increased coordination and cooperation between the public and private sectors. See recommendations 2, 13, and 17.

- *"Improve Security Awareness":* Develop national exercises that measure U.S. ability to prevent and respond to terrorist attacks, including scenarios in which attacks are directed at military mobilization or critical infrastructure within U.S. ports and waterways. The Departments of Transportation and Defense and the FBI should assume responsibility for this recommendation and coordinate with other agencies and public and private sector stakeholders.

  Comment: As discussed in Chapters 4 and 5 within the context of securing the nation's militarily Strategic Seaports, the Seaport Commission strongly supports the development of national exercises to prevent and respond to terrorist attacks in our nation's seaports. See recommendation 16.

- *"Identify Vulnerabilities and Improve Transparency":* Conduct baseline and periodic reviews of the strategic ports and waterways of the National Port Readiness Network to identify vulnerabilities and determine the readiness of public and private resources to meet military mobilization requirements.

  Comment: As discussed in Chapters 4 and 5, the Seaport Commission strongly supports baseline and periodic vulnerability and threat assessments for each major U.S. seaport including the militarily strategic seaports. See recommendations 7 and 16.

- *"Identify Vulnerabilities and Improve Transparency":* Conduct readiness exercises that test the ability to support continued waterside security and uninterrupted military mobilization operations

while responding to (1) terrorist threats and acts and (2) nontraditional asymmetrical attacks on the Marine Transportation System.

Comment: As discussed in Chapters 4 and 5, the Seaport Commission strongly supports the development of readiness exercises to deter terrorist attacks and to respond to nontraditional asymmetrical attacks on our nation's seaports. See recommendations 7 and 16.

- *"Identify Vulnerabilities and Improve Transparency":* Develop and integrate real-time intelligent systems for tracking cargo, personnel, and vessel operations throughout the Marine Transportation System.

  Comment: As discussed in Chapter 7 *(Intelligence and Information Management),* the Seaport Commission supports development of an integrated, real-time information system for tracking the movement of vessels (including cargo and personnel) within the seaport environment. See recommendation 18.

- *"Forge Stronger Public/Private Partnerships":* Advocate and oversee integration of public/private sector national security strategy, policy, and goals to support Department of Defense mobility plans.

  Comment: As discussed in Chapters 5 and 6, the Seaport Commission strongly supports increased public/private coordination to support Department of Defense mobility plans. See recommendations 13, 16, and 17.

- *"Forge Stronger Public/Private Partnerships":* Develop public/private sector Marine Transportation System partnerships to establish security guidelines for onshore facilities, offshore facilities, and vessels, and implement incentive-based mechanisms to address Marine Transportation System security vulnerabilities. The Interagency Committee for the Marine Transportation System and regional and local coordinating bodies should be engaged on this issue. Participants should include the Coast Guard, Department of Defense, Maritime Administration, Customs Service, private sector organizations, state and local authorities, and labor organizations.

  Comment: As discussed in Chapters 5 and 6, the development of security guidelines via public/private sector partnerships is one of the key Seaport Commission recommendations. See recommendations 13, 14, and 17.

- *"Strengthen International Cooperation":* Develop a strategy and process for advancing U.S. operating guidelines and minimum security standards on an international basis; and provide intelligence and training to improve international oversight of the global maritime infrastructure.

  Comment: As discussed in Chapter 8, the Seaport Commission strongly supports stronger international cooperation due to its potentially positive impact on domestic seaport security. See recommendation 19.

Ocean Policy Study, September 1999

In June 1998, President Clinton directed the Cabinet to provide him with recommendations for a coordinated, disciplined, long-term federal ocean policy. Although the report covered many areas, the two that are most relevant to this study were on marine transportation and maritime enforcement. These are the ongoing concerns stated in the report:

- Many federal agencies, state and local governments, port authorities, private industries, and labor groups share responsibility for managing safety, security, and environmental protection, which makes coordinated responses to challenges and opportunities very difficult to achieve.

- Innovative U.S. financing, regulatory changes, and tax mechanisms may be

required over the long run to spur the substantial public and private investment needed to meet growing demands.

- The marine transportation system infrastructure and supportive information systems may be stretched to their limits to cope with projected increases in the system's users and the size, speed, and diversity of vessels.
- Growth in vessel traffic will increase risks to sensitive ocean, coastal, and inland environments.
- International criminal and terrorist threats are constantly changing and adapting to current law enforcement capabilities. Today's communications and integrated intelligence systems lack the sophistication to support real-time monitoring of vessels, people, and cargo movements.
- High-level awareness of the emerging threats to maritime transportation is required, as is interservice, interagency, and international cooperation to address them.

The resulting September 2, 1999, report—entitled *Turning to the Sea: America's Ocean Future*—covered many areas, but the ones most relevant to seaport security were on marine transportation and maritime law enforcement. Specifically, the pertinent recommendations from these two areas are listed below—all of which are strongly supported by the recommendations found in this Seaport Commission final report.

- *Marine transportation:* Facilitate coordination among all stakeholders by establishing a federal Interagency Committee for the Marine Transportation System, a nonfederal Marine Transportation System National Advisory Council, as well as regional and local committees.
- *Marine transportation:* Meet national security objectives by balancing commercial demands with safeguards and inspections to protect against security threats and support military mobilization.
- *Maritime law enforcement:* Improve cooperation at the interagency, interservice, and international levels to address threats to our maritime interests, including collecting and sharing key information, and developing and integrating real-time intelligence systems for tracking cargo, personnel, and commercial vessel operations.
- *Maritime law enforcement:* Improve U.S. capability to conduct surveillance, detection, identification, classification, and interdiction of maritime threats before they reach U.S. coasts and harbors.
- *Maritime law enforcement:* Acknowledge the low level of current security awareness in the marine transportation system, and initiate a national education campaign to improve federal, state, and local awareness of the growing threats.

Roles and Missions of the Coast Guard, January 2000

In March 1999, President Clinton issued an Executive Order creating an Interagency Task Force on the Roles and Missions of the U.S. Coast Guard, to provide advice and recommendations on the appropriate roles and missions of the Coast Guard through the year 2020. The task force included representatives from the Coast Guard, the Departments of Transportation, State, Defense, Justice, Commerce, and Labor, the Environmental Protection Agency, the Nuclear Energy Commission, the Office of Management and Budget, the National Security Council, the Domestic Policy Council, the Council on Environmental Quality, the Office of National Drug Control Policy, and the Office of Cabinet Affairs.

The report relevance is its reaffirmation of the mission of Coast Guard to continue in national defense, including port security, and at-sea drug interdiction. The report

was issued in January 2000 and contained the following overarching conclusions:

- The Coast Guard's roles and missions support national policies and objectives that will endure into the 21st century.
- The U.S. will continue to need a flexible, adaptable, multi-mission, military Coast Guard to meet national maritime interests and requirements well into the next century.
- In order to hedge against tomorrow's uncertainties, the Coast Guard should be rebuilt so as to make it adaptable to future realities.
- In keeping with its well-deserved reputation as one of the federal government's most effective and efficient organizations, the Coast Guard should continue to pursue new methods and technologies to enhance its ability to perform its vital missions.
- The recapitalization of the Coast Guard's Deepwater capability is a near-term national priority.
- The Deepwater acquisition project is a sound approach to that end and the Interagency Task Force strongly endorses its process and timeline.

Maritime Drug Trafficking Project, Ongoing

The Coast Guard requested the National Drug Intelligence Center (NDIC) to conduct a study of the top 10 to 20 maritime drug trafficking organizations that pose a threat to the United States, covering the identities of the vessels used, key transportation personnel, modes of operation, and the traffickers' reactions to Coast Guard interdiction efforts. Among the critical questions to be studied are:

- Fully identify the most significant drug trafficking organizations transporting drugs to the United States by non-containerized maritime means, including only those that control the means of transportation.
- Fully identify the airborne and seaborne assets used to transport drugs to the United States by maritime means.
- Determine how drugs are transported to the United States by maritime means.
- Describe how the organizations react to Coast Guard interdiction efforts.

Field visits included in the study cover Boston, Buffalo, Charleston, Chicago, Cleveland, Detroit, Duluth, Houston, Galveston, Jacksonville, Key West, Long Beach, Miami, Mobile, New Bedford, New Orleans, New York/New Jersey, Norfolk, Philadelphia, Pittsburgh, Port Everglades, Portland (Oregon), San Diego, San Francisco, San Juan, Savannah, Seattle/Tacoma, Tampa Bay, Vancouver, and Wilmington.

The information responding to this task is relevant as the Commission makes interagency operational recommendations.

State of Florida, Office of Drug Control Statewide Security Assessment of Seaports, Ongoing

The state of Florida's Office of Drug - Control is in the process of a broad, comprehensive assessment of security (and related issues) at the state's 14 deepwater ports. This complete, objective assessment is to develop a viable campaign plan to implement enhancements that solve drug interdiction, money laundering, and general port security problems. Currently there is an on-site data collection for the assessment to address physical security, port operations, and information security. The stated focus of the study is:

- Discovery and interdiction of illegal drug imports.
- Discovery and confiscation of illegal exports of cash.
- Reduction or elimination of cargo theft.
- Safety and security of persons working at ports.

The study topics clearly have relevance to the work of the Commission. In fact, the commitment of the State of Florida seems to offer an opportunity to prototype many of the items listed in the Model Port Concept in Appendix F.

Appendix D: Comments from the Private Sector and Other Stakeholders

Chapters of this report have discussed the full range of issues related to the security of U.S. seaports. Although this report discussed the views of the seaport stakeholders from time to time, those chapters did not focus on them. Because the private sector, port authorities, and other levels of government are so critical in the operations at seaports, the Commission wanted to use this appendix to highlight their issues. In fact, the President's memorandum initiating this study specifically stated:

> In the course of its work, the Commission shall seek input from, and take full account of, the expertise and views of the many different state and local government agencies with relevant responsibilities, as well as the involved private sector interests.

The Commission solicited comments by talking to hundreds of businesses involved in seaport operations; surveying 12 seaports and talking with officials and workers in each port; soliciting comments in a *Federal Register* notice; holding public hearings in three locations; meeting with national industry groups; and attending and participating in national conferences whenever and wherever they were held.

The Commission found that stakeholders in seaports have a wide range of interests and views about the issues involving crime and security, and that the issues involving port security and/or the lack of security within U.S. seaports affect stakeholders in a variety of ways.

The various stakeholders and their interests were described in Chapter 2, as a means of setting the full seaport scenario for readers of this report. Throughout the report, references are made to specific concerns and interests that stakeholders expressed to the Commission and that the Commission took account of in developing its findings and recommendations. To complete the record, this chapter adds summaries of comments heard from the various stakeholders at focus group sessions, in public hearings, and in written comments to the Commission.

Focus Group Sessions

The Commission made extensive efforts to reach out to organizations and entities by holding a total of 46 focus group sessions with representatives from the trade during on-site surveys at the ports of Charleston, Gulfport, Long Beach, Los Angeles, Miami, New York/Newark, New Orleans, Philadelphia, Port Everglades, San Juan, and Tacoma. Focus groups were held with port authorities and terminal operators; vessel operators and carriers; trucking companies and warehouse operators; rail carriers; importers, exporters, and freight forwarders; customs house brokers; organized labor; and miscellaneous trade groups.

When soliciting comments, the Commission specifically asked the stakeholders to describe problems that need to be solved concerning crime, terrorism, and security in seaports; any proposals for new laws or regulations; suggested methods for ensuring better reporting and more accurate collection of data; and possible ways to

improve coordination and cooperation among government agencies.

A review of the focus group meetings revealed that there is no consensus on how to address most security issues. The following significant and recurring issues and recommendations were raised by stakeholders at these sessions.

Port and Terminal Security

Carriers and terminal operators in one port were concerned that security improvements in the port were taking too long. A carrier in another port expressed his concern about the lack of security in the port during operation "Desert Storm." Carriers and labor, as well as a cruise line operator, felt that the ports they operated in were vulnerable (to criminal and terrorist activities). Carriers in some ports and brokers/freight forwarders in another port also felt that there was a need for nationwide minimum standards for ports, that port security practices should be standardized, and that someone (undetermined) needs to address non-uniformity between ports. Carriers and terminal operators in two ports were satisfied with the security in the ports in which they operated. There was also concern that the presence of security guards within some ports was inadequate and that the "personnel" security practices of some transportation firms were insufficient to prevent crime.

There was much discussion about minimum security standards. Some members of the private sector have suggested developing and publicizing the "standards" and components that constitute acceptable security practices in a port and that could serve as the basis of a "model" port that seaports around the country could emulate. These guidelines in the "model" port could include such elements as adequate physical security (lights, fences, etc.), access control (gates, identification cards, etc.), personnel (employment and criminal history checks, polygraphing, and fingerprinting), and procedural (cargo receipt and delivery systems) standards in a seaport. The majority of the commenters favored some sort of national standards, but there were a variety of opinions on whether these standards should be mandatory or voluntary. A representative of a labor organization who worked in one port suggested that there should be federally mandated security standards tailored to the needs of individual terminals. A representative of a labor organization who worked in another port felt that there should be minimal federal government involvement in port security.

The standards, or components, that make up a "model" seaport and a "model" cargo release system could be jointly developed by government and the private sector, and the trade community would be encouraged to adopt these standards and components, some commenters suggested. In addition, the private sector and government could decide to designate one seaport in the United States as a "model" pilot seaport, and work jointly with personnel in that seaport to implement the acceptable standards and components that they have identified.

At one meeting, the private sector suggested improvements to ports that could enhance overall security within an individual port or address security issues common to many ports. The suggestions included creating "port security" yards within seaports where containers could be stored adjacent to terminals facilities; segregating processes such as cargo and passenger operations within ports; and reconfiguring traffic patterns in seaports to reduce opportunities for the criminal elements in ports to gain access to sensitive areas. Truck and rail firms at two ports expressed their support for establishing "port security yards" within ports for the safekeeping of containers, and for enhanced "sealing" practices within the port. Carriers and terminal operators at one port also suggested the need to segregate processes (cargo and passenger) in the port as a means of enhancing security

within the port, and members of a trade organization in one port also thought the traffic patterns in the port needed to be reconfigured.

The trade community in one port and brokers/freight forwarders in another expressed concern that security costs should be reasonable, and that increased security measures should not negatively affect the flow of commerce.

Carriers in one port felt that government agencies that have "partnership-type" programs with the private sector needed to expand these programs to U.S. seaports. A labor organization in another port recommended that federal agencies develop local and national "partnerships" with labor organizations as a way to foster communication and information-sharing.

A carrier in one port and a cruise ship operator in another port felt that "labor" in the ports represented a "risk" to operations. The trade in another port felt that getting union members to comply with port procedures was often an issue. Labor in one port and carriers in another port felt that "transient" labor (truck drivers or "day" workers) was a major unresolved issue in the port.

Carriers and terminal operators in one port thought that "information" about shipments is sometimes "too available." They felt that this availability could facilitate criminal activities.

A member of the trade also suggested that seaport users adopt an "integrated security system" that his firm employs, which makes internal conspiracies harder to perform during cargo/container drop-off and pick-up. The system, which can be added to a firm's existing receipt and delivery procedures, restricts the movement of drivers and rotates employees assigned to delivery and receipt operations.

The issuance of identification cards to dock workers and port employees was found to be a highly sensitive issue. Some of the carriers, terminal operators, cruise line operators, and trade thought that the issuance of identification cards was a good idea and that there should be standardized/universal cards for the trade to use (especially in Florida). Carriers and terminal operators in another port also expressed their concern about knowing who belongs in ports. Some members of labor unions were in favor of identification cards, while others were strongly opposed. Some union officials saw identification card requirements as an invasion of union members' privacy. Others said identification cards were unnecessary because each union member had a union card in his pocket that could be produced if necessary. Others said that the union members were well-known on the port and identification was not needed. One union official also commented that the wearing of identification cards at the seaports was a negotiable issue between the port authorities and workers and that the government should not interfere.

Some members of labor unions, railroads, and trucking firms expressed concern about implementing identification card programs and the practicality of issuing the cards at the port level, especially to transient workers, railroad employees, and truck drivers. A member of one trade organization thought it would be beneficial to have a nationwide identification card program.

The performance of background/criminal history checks on dock workers and port employees was clearly the most controversial issue raised by the stakeholders. Most comments we received from labor groups dealt with their strong opposition to imposing requirements for background checks and criminal record checks on labor. They felt strongly that they were not the problem with crime at the seaports and should not be singled out. They considered any such program to be a violation of their privacy. Programs with these basic characteristics were implemented in both Port

Everglades and Miami over the objections of the union. In Miami, the labor union was able to negotiate a role in reviewing the circumstances that barred a union member from employment at the port on a case-by-case basis. In Miami this seemed to be acceptable to the union.

Other stakeholders (including a Gulf Coast labor group) saw benefits in having background checks performed on employees, and wished to see the checks expanded to other workers. At two ports, terminal operators and carriers were in favor of background checks for port employees, and during one focus group session, truck and rail company personnel voiced their support for identification card programs that could control access to the ports and its terminals.

Carriers and terminal operators in one port felt that there was a lack of awareness on the part of some elements of the trade community regarding security matters, and a carrier in another port suggested that law enforcement personnel could benefit from training on shipping and related industries. Labor in one port suggested that training for security guards was inadequate. A cruise line operator suggested that the federal government should sponsor a port security course at least once a year in South Florida.

Law Enforcement

The "threat" of terrorism was a concern to cruise line operators, carriers, and terminal operators in two ports. Importers/exporters and carriers in one port also felt that there was a need for more coordination and planning to address possible terrorist threats and incidents in ports and that there was a need to increase the trade's awareness of terrorism and terrorism-related intelligence.

Carriers, terminal operators, brokers/freight forwarders, and truck and rail firms in several ports expressed their belief that federal resources are lacking at the seaports, that federal and local police are lacking on the piers and terminals at seaports, and that law enforcement's response is often poor, or nonexistent, in the seaports. In order to address this issue, the carriers and terminal operators at several ports, labor at one port, and rail and trucking companies at another port suggested increasing federal resources at the seaports and increasing the presence of federal and local police on the piers and terminals at seaports.

Several of the carriers and terminal operators in one port saw a need to share information about cargo theft, at both the port and national levels, to increase penalties for cargo thefts, and to create and fund cargo theft task forces as appropriate. Rail and truck firms in one port recommended that "cargo crime" should be included as a category in the FBI's Uniform Crime Reporting, and a truck/rail firm in another port thought that the trade could benefit from sharing information about cargo losses among each other.

In two ports, carriers and terminal operators expressed their views that violators were not being punished sufficiently for criminal activities (especially cargo theft), and they recommended that penalties and sentencing guidelines for violators be increased as possible solutions to these issues.

Carriers, cruise line operators, and terminal operators at one port and the trade in another port felt that coordination and cooperation were lacking between law enforcement agencies, the ports, and their tenants and between the trade within the ports, especially with respect to issues relating to terrorism and cargo theft. These stakeholders suggested that law enforcement agencies should cooperate/share information more in the port, especially about terrorist and cargo theft issues. The trade in another port suggested establishing a "port tenant" committee as a way to help define security-related roles and responsibilities in the port.

Members of the private sector thought that government and the private sector should find ways to work together to improve security within seaports. The ports of Port Everglades, Jacksonville, and Gulfport currently have government/ private sector initiatives to enhance security within their ports.

Private sector commenters cited the need to develop and maintain partnerships at the national and local levels between government agencies and the members of the private sector (such as ports and labor unions). The partnerships would serve as ongoing forums to increase communication between partners and address security-related concerns within the ports.

Members of the private sector also felt that additional communication between principals (carriers, terminal operators, port authorities, etc.) in ports would be beneficial. Examples of cooperation would be the establishment of port tenant committees that could meet locally to identify and address security concerns, sharing of information with other principals about losses and incidents through local forums, and establishment of a local theft-tracking database for the port.

Federal Inspection

The carriers and terminal operators in one port and the brokers/freight forwarders in another port recommended that centralized facilities be created in ports where all federal agencies can perform their examinations. Labor organizations in two ports felt that all devanning/stripping of containers should be performed on the piers.

Carriers and terminal operators in several ports stated that the acquisition of technology (such as X-rays and closed circuit television) could assist law enforcement personnel in processing cargo and detecting violations. The trade representatives at one port and the carriers in another port both recommended that information systems like the automated system used by Customs be funded. Truck and rail carriers in two ports thought that the trade needed to acquire and use "smart card" technology and "scanner" technology to enhance security within their operations. Carriers and terminal operators in one port also thought rail cars need to be built to reduce their vulnerability to theft and pilferage.

In many of the ports the trade endorsed the use of technology and equipment to deter/prevent cargo and equipment thefts, track cargo and conveyances, and detect contraband. The equipment/technology that the trade supported using included electronic seals, cargo tagging/tracking systems, antitheft devices, smart card technology, X-ray systems, and cameras. In one location, the trade also suggested that the government and private industry underwrite a study of technology to determine what systems should be employed in seaports and how they can be best used.

Written Comments Received from Stakeholders

This section of the report summarizes written comments received in response to the Commission's notice, published in the *Federal Register,* dated June 16, 1999. The notice requested comments over a 60-day period from interested parties on the issues of crime in seaports, terrorism and environment crimes, security and prevention, cargo control and technology, and possible legislative initiatives. In response to the notice, the Commission received written comments from 13 organizations and individuals. The following is a synopsis of the written comments received.

The American Association of Port Authorities wrote to the Commission on August 9, 1999, with comments covering the following four areas: (1) The Customs Service should join with the Drug Enforcement Administration and the FBI in developing a proactive policy and program that shares criminal intelligence with state and

local law enforcement agencies. (2) The Departments of Defense, Transportation, and Justice should support and participate in the efforts to review the wartime vulnerability and peacetime security needs of U.S. ports. This review should be coordinated with all relevant federal (military and civilian), state, and local law enforcement and security-related agencies, including public port authorities. Upon completion of the assessment, a concerted effort should be undertaken to remedy any discrepancies and other security deficiencies identified in the process. (3) The state and federal governments should provide appropriate legal and/or legislative support in assisting the private contract security guard industry in its efforts to protect the nation's cargo commerce with security personnel of the highest caliber and integrity. (4) Sentencing for cargo theft crimes under federal law should be strengthened, a national database with information about cargo theft should be established, and a centralized office should be created within the federal government to oversee efforts designed to curb cargo theft and increase coordination with the private sector and state and local law enforcement.

The Commission also received a concept paper from the new **Chairman of the Security Committee from the American Association of Port Authorities** on June 4, 1999. He recommends that a Maritime Security Institute be established and funded as a joint project between the public and private sectors. The Institute would establish a forum where students take courses of instruction in conducting security surveys, developing security plans, implementing security measures, and other security-related programs. He suggested Miami as the location for this institute.

The National Cargo Security Council wrote to the Commission on August 13, 1999, with the following suggestions: (1) The scope of the Commission's study should be expanded to look at terrorism, cargo theft, narcotics, and internal conspiracies, and to look outside the traditional port limits. (2) The study should look at the ports as a major component of a larger intermodal system and look at the criminal activity that occurs outside the direct control of ocean carriers/ports. (3) The Commission should issue guidelines for identification standards for the various parties normally in port areas or handling cargo, such as port management, labor, truckers, and carrier personnel. (4) A model should be developed (acceptable to law enforcement, Customs, and the industry) that articulates a secure cargo delivery process. (5) The Commission should increase sentencing guidelines. (6) The Commission should create seaport crime as a category in the "Uniform Crime Reports." (7) The Commission should establish a national database for cargo crimes and fund multiagency cargo crime task forces. (8) The Commission should "partner" with the private sector in efforts to address seaport crime, and law enforcement should attend seminars presented by the industry on seaport/cargo operations and security to learn how these businesses work.

The **International Longshoremen's and Warehousemen's Union (Southern California District Council)** wrote to the Commission on August 8, 1999, that it believes that petroleum tankers, refineries, rail operations, containers, vessels, and trucks all pose threats for possible terrorist activities. The union also said container storage, transfer, and marine terminals are vulnerable to criminal activities. It felt that white-collar crimes are prevalent in ports and that security guards used in ports and for terminals must be sufficient in number and receive proper training. The union believes that physical security and lighting is important for seaports. It expressed opposition to any propositions to privatize the port's work force now protected by union contracts and to perform background checks on longshoremen.

The **International Longshoremen's Association** wrote to the Commission on August 12, 1999. It believes the association has the ability to detect terrorism, environmental offenses, and breaches of security, and it recommended that guidelines be developed for use by its members to assist them in recognizing and reporting criminal activities involving movements of drugs and contraband, and potential acts of terrorism.

The **International Longshoremen's and Warehousemen's Union (San Francisco)** wrote to the Commission on September 16, 1999. It said it was opposed to criminal background checks being performed on its members. It said the wearing of identification badges is unnecessary, and any requirement to wear them should be negotiated between the employer and the union. It expressed a need for additional guards at the ports, and it supported the adoption of a law mandating manning and training requirements for guards.

The **International Longshoremen's and Warehousemen's Union-Local 24 Puget Sound Council** wrote to the Commission on August 1, 1999, and expressed opposition to HR 318, the "Shaw Resolution," which would require that criminal history checks be performed on dock workers in seaports.

The **Transportation Trades Department, AFL-CIO** sent a letter to the Commission on August 16, 1999, expressing opposition to criminal background checks being performed on port workers and related employees. It encouraged the Commission to create a set of recommendations that will recognize the role labor can play in reducing crime and criminal activities at U.S. seaports.

H&M Terminal Transport wrote to the Commission on August 16, 1999, with four recommendations and a comment. (1) The Sealink card system, which gives authority in New York/New Jersey for drivers to pick up loads for specific trucking companies, should be refined. (2) Federal agencies need to look at investigating crimes with smaller thresholds (less than $100,000). (3) Electronic delivery orders for the port of New York/New Jersey should require a back-up order from trucking companies to pick up freight. (4) The industry needs to safeguard information from thieves. It also commented that cargo theft informants are often involved in the theft/distribution/fencing chain.

The **American Institute of Marine Underwriters** wrote to the Commission on August 10, 1999, with four recommendations: (1) A centralized database on cargo theft information needs to be developed. (2) Penalties, jail time, and fines need to be increased for persons convicted of cargo crimes. (3) Background and security checks need to be performed on all new hires directly involved in the transportation of cargo. (4) An international network of law enforcement agencies should be established to coordinate efforts to combat cargo crimes.

The South Carolina Ports Authority wrote to the Commission on August 23, 1999. It said it wanted to see realistic goals set for seaport security that neither constrain the flow of commerce nor create additional costs for ports. It said that background checks (on non-port authority personnel) should not be done without probable cause. It expressed concerns that establishing a visitor pass or identification card program for truck drivers entering the port would be inefficient and costly.

Barry Tarnef wrote the Commission on August 12, 1999. He said he wanted to see intermodalism incorporated into the Commission's study. He suggested that nonfederal law enforcement personnel should serve on the Commission, because of their expertise in transportation-related crimes, and that the Commission should work to reduce all types and levels of crime. He also expressed support for the Cargo Theft Deterrence Act of 1999. He opposed the

adoption of the cargo theft database (TIPS) program, and said a national "cargo theft" database is necessary. He believed that the "known shipper" initiative that is used in the air environment to identify the contents of a shipment and ensure proper manifesting might have applications in the sea environment. He said that more emphasis should be placed on law enforcement training at the local, state, and federal levels, and that law enforcement personnel need to be linked electronically.

Representatives from **FLIR Systems** wrote to the Commission on August 17, 1999, that the thermal imaging systems it markets might have applications for law enforcement agencies that have responsibilities in the seaports.

Public Meetings

The Commissioners held three public meetings/listening sessions to receive input and feedback from the private sector on the significant issues involving crime, security, and terrorism in U.S. seaports. The sessions were held in the Norfolk/Hampton Roads area on February 2, 2000; the San Francisco/Oakland area on February 16, 2000; and the Houston area on March 1, 2000. During the course of the meetings the Commissioners provided the public with some of the observations seen during their on-site seaport surveys, and sought private sector solutions and recommendations for addressing issues related to crime terrorism and security in seaports.

Norfolk/Hampton Roads, Virginia

The first public meeting/listening session held in the Norfolk/Hampton Roads, Virginia,, area on February 2, 2000, was attended by representatives from trade associations such as the National Cargo Security Council, the Hampton Roads Maritime Association, and the Carriers Container Council, Inc. In addition, there were representatives from vessel carriers, port authorities, and customhouse brokers in the Hampton Roads area, and private consultants from the field of security and loss prevention.

During the session, the following areas were discussed: the government's role in seaports, the use of identification cards and background checks to control/restrict access to ports, crimes in seaports, the lack of information about shipments, security enhancements within ports, security standards for seaports, and security for information systems which service seaports.

The trade community believes that the federal government has a significant role in seaports, especially concerning the placing of technology in seaports, the investigation of crimes, and the ability to control entities (carriers, etc.) that use seaports. Some of the attendees felt that government needed to make a bigger commitment for law enforcement agencies within ports and that the federal law enforcement community needed to work more in partnership with the trade community within ports and to share information.

The subjects of identification cards and background checks for employees who require access to seaports were discussed extensively at the session. Many of the speakers said that the use of an identification card program for our nation's seaports was a good idea, and that cards could increase accountability within a port and uniformity among ports. There was no clear consensus, however, about "who" should have identification cards in ports, whether there should be "standardized or universal" port identification cards for all U.S. ports, and whether there should be national standards requiring criminal history checks for all employees in seaports. One presenter stated that the government should help determine who within a seaport requires an identification card, and that the port, not the terminal operator, should actually issue the cards. Another presenter also stated that if organized labor is

required, with all workers, to receive identification cards, and the program is uniformly and fairly administered, it will work.

The issue of crime, and especially cargo thefts, in seaports was widely discussed. A presenter estimated that $10 billion in losses occurs each year in the United States because of cargo thefts. While there is the opinion that most cargo thefts occur outside seaports, but within close proximity of the ports, there was also an acknowledgement on the part of a presenter that seaports and seaport users are often reluctant to report crimes because it could be bad for business. The attendees advised the Commission that it should be the responsibility of the government, not insurance companies, to collect and manage data about cargo losses. The trade also felt that the federal government should address the issue of cargo thefts by funding and creating more multi-agency task forces that address security concerns, collecting information and intelligence about crimes, and updating cargo crimes statutes and sentencing guidelines. There was a concern on the part of the trade that alien smuggling, especially via containers, is significant in the maritime environment, and seaports are vulnerable to terrorist-related incidents.

The issue of security "standards" for seaports and seaport users was a central topic at the meeting. Presenters advised the Commission that they would like to see guidelines about security measures developed and recommended, but that the guidelines should not be mandated by government agencies. An alternate approach that was discussed was having the government set the guidelines regarding security that the industry (including carriers, ports, and terminals) could follow as part of a partnership program. Once the guidelines are established, the market forces would then work to encourage ports, and the ports' users, to comply with the guidelines.

There was the sentiment at the meeting that many ports could adopt security enhancements without significantly increasing costs, and that by adopting these enhancements they could reduce their insurance costs. Presenters expressed their views that more modern inspection techniques by federal agencies in ports and funding for non-intrusive detection technology (capable of scanning containers and other large articles) could make seaports more secure and enable law enforcement agencies to detect crimes more effectively.

The issue of unreliable manifest information about shipments was discussed briefly at the meeting. A representative of a vessel carrier advised the Commission that shippers, not carriers, need to increase their compliance about accurately describing shipments. Two members of the trade also expressed their support for continued funding for Customs automated data systems.

Concern was expressed at the session about the possible vulnerability of the information technology systems that service ports and the need for intelligence and information-sharing about possible threats to critical areas in ports such as power, electrical, and data systems. A presenter advised the Commission of the benefits of analyzing a port's "cyber" systems and conducting a critical dependency analysis of ports so that vulnerabilities can be identified and addressed before they are exploited.

In summation, the members of the trade community who attended the Norfolk session believe that the federal government has a significant role in seaports. In general, they supported the use of identification cards to control access to seaports, but there was no agreement on who should be required to have, or issue, the cards. The trade believes that cargo thefts at seaports, and environs, are a major issue that can be addressed by funding and creating more multi-agency task forces, collecting information and intelligence about crimes, and updating cargo crimes statutes and sentencing guidelines. The trade voiced

support for establishing security guidelines and enhancing security practices within seaports, for increasing the trade's compliance of imported merchandise, and for supporting Customs' automated data systems.

San Francisco, California

The second in the series of three public meeting/listening sessions was held in San Francisco, California, on February 16, 2000. The session was attended by representatives from the National Cargo Security Council, the Maritime Security Council, the National Brokers and Freight Forwarders Association, the American Institute of Marine Underwriters, and the American Association of Port Authorities. In addition there were representatives from the International Longshoremen's and Warehousemen's Union, vessel carriers, port authorities, stevedoring companies, various West Coast ports, terminal operators, insurance companies, warehouse operators, consultants in the field of security, and the general public.

The following significant areas were discussed: the role and requirements of government's agencies in seaports, the vulnerability of seaports to crime and terrorist-related incidents, the need for information and additional legislation for export shipments, the need for data about cargo thefts, security standards for seaports, the use of identification cards and background checks to control/restrict access to ports, the lack of information about shipments, and security enhancements within ports.

Senator Diane Feinstein spoke at length and advised the Commission that the following is needed at seaports: additional technology, increased coordination between federal, state, and local law enforcement agencies, increased federal oversight of seaports, additional Customs and Immigration officers, additional Customs and Commerce investigators, partnerships with trade and labor, and implementation of counterterrorism techniques at seaports. She also felt that, to address cargo theft issues, port authorities should be responsible for tightening and standardizing security operations within ports, and she expressed a willingness to work with the Commission to come up with appropriate legislation and recommendations to support the work of the Commission.

The issue of crime and especially cargo thefts, was widely discussed at the session. The crimes cited by attendees as occurring at seaports included auto and cargo theft, as well as alien, drug, and contraband smuggling. Some in attendance also believed that seaports were vulnerable to acts of terrorism and weapons of mass destruction. In order to address the threat of terrorism, it was suggested that a systematic approach to improving security at seaports was required.

Regarding the issue of cargo theft, two of the presenters felt that thefts occurred frequently outside, not inside, the ports or while in transit between businesses. A presenter stated that a criminal's knowledge about shipments could facilitate cargo thefts within a port or its environs, and that the lack of significant penalties for cargo theft (as compared with drug smuggling) makes cargo theft more attractive to organized crime. Two of the presenters also stated that the lack of a uniform database to collect information about cargo theft losses makes estimating industry losses difficult and that law enforcement's coordination of cargo theft data needs to be improved. A centralized database for capturing cargo theft data, the inclusion of "cargo theft" as a category in the Uniform Crime Reporting, and increased penalties for cargo theft crimes were suggested as a means of addressing these issues. A presenter offered to assist government agencies in developing the database.

The issues of the need for reliable and accurate information about export shipments and the government's need to raise

the compliance of the trade regarding exports were central topics at the meeting. The presenters suggested the mandatory use of the Customs Automated Export System, educating the trade about export requirements, and increased penalties for violators as ways to increase compliance.

The most discussed issue at the session concerned the use of identification cards and background (criminal history) checks to control/restrict the access of employees to seaports. Members of organized labor who spoke were opposed to the concept of using identification cards and background checks to control access to seaports. They stated that crimes were not being committed by dock workers at West Coast ports and therefore that identification cards were unwarranted. They said that any recommendations (like identification cards) could negatively impact the viability of commerce on the west coast. They expressed concerns that identification card programs could delay "transient or casual" laborers (who are sometimes used in ports during busy times) from being able to get to work sites. In addition, they felt that it is impractical to attempt to identify "sensitive zones or work areas" in ports where additional security (and therefore identification cards and a stable work force) could be used on ports.

Some members of trade organizations who spoke at the meeting expressed support for the use of identification cards and background checks, although there was no clear consensus about who should issue the cards or if they should be mandated. One opinion was that the government should mandate the cards, and the ports should issue them. Another member of the trade felt that identification cards, but not background checks, should be required for all workers who require access to seaports. A third presenter believed that identification cards were only effective if combined with adequate physical barriers such as fences.

The issue of security standards for seaports was a central topic at the session. Some members of the trade believed that minimum standards were warranted for seaports, while others felt that "guidelines" (which would not take regulations to implement) were more appropriate. Some presenters expressed concern that if state or local governments issued standards it might result in 50 disparate standards. One presenter advised the Commission that he was unsure what the role of the federal government should be in the issuance and development of standards.

Some members of the trade expressed their views that security, and anti-crime initiatives, could be enhanced at seaports and facilities within seaports through the use of technology, the increased presence of uniformed officers (federal and private security) at seaport facilities, increased examinations, and through better control of documentation and cargo.

In summation, the trade and members of the public who attended the session in San Francisco were concerned about crime in U.S. seaports and believe seaports to be vulnerable. However, they believe that crime in seaports can be addressed by enhancing security practices, by placing additional federal resources and technology in seaports, as well as by increasing information about shipments and increasing compliance on the part of the trade. They believe that cargo theft (at seaports and environs) is a major issue that can be addressed in part, by better data collection and increased law enforcement coordination. Although organized labor is opposed to identification cards and background checks as a means of controlling access to seaports, other members of the trade voiced their support for both identification cards and background checks. The members of the trade also supported minimum security guidelines for seaports.

Houston, Texas

The third and final in a series of three public meeting/listening sessions was held in Houston, Texas, on March 1, 2000. The session was attended by representatives from the oil industry, railroads, carriers, terminal operators, freight forwarders, stevedoring companies, maritime associations, congressional staffers, the press, local law enforcement agencies, representatives from the Ports of Houston, Texas City, and Galveston, and the general public.

The following significant areas were discussed: cargo theft in seaports, the sharing of information in seaports, identification card systems, security standards and technology for seaports, partnership between government agencies and the trade, controlling access to seaports, and the role of the federal government in seaports.

The issue of crime and especially cargo thefts was discussed. The main crimes that occur at seaports were identified as drug smuggling, cargo thefts, and terrorism. One of the presenters felt that cargo thefts occurred most frequently when goods were in transit or while being shipped, and that her company's product line (high-tech products) was vulnerable to thefts because the product could be easily disposed of by criminals, and information about shipments could be easily obtained. She also stated that losses are increasing each year in her industry (an estimated $1 billion in losses last year) and that organized crime is now involved in thefts. The presenter felt that a uniform database to collect information about cargo theft losses is needed, companies need to be adequately compensated (by insurance companies) for losses, federal guidelines for sentencing criminals involved in cargo thefts need to be developed, and current penalties for cargo theft violations are insufficient.

There was also significant discussion about the need to share information about losses. Presenters stated that information-sharing needed to be enhanced between ports and tenants, between law enforcement agencies and the trade, and between security people in related industries.

The use of identification cards to control/restrict the access of employees to seaports was raised at the meeting. One presenter stated that identification card systems needed to be uniform for all ports and that all employees (drivers, dock workers, etc.) who required access to seaports should be required to obtain the cards. The presenter also felt that the use of the cards could facilitate, not hamper, commerce within seaports. However, one speaker expressed concern that the requirement for prospective employees and workers to have identification cards could adversely affect the ability of emergency response teams to access some seaports.

There was also some discussion about performing background checks on employees who apply for identification cards and the drug testing of employees at seaports. One presenter felt that the performance of background checks could deter criminal activity in seaports and another speaker expressed support for random drug testing of seaport workers.

The issues of security standards for seaports and controlling access to seaports were central topics. One presenter was receptive to identifying security guidelines for ports, but stated that government should not mandate strict standards for all ports. He felt that standards should be developed with a view to the needs of commerce in each individual port and the various industries (oil refineries, bulk merchandise importers, etc.) that make up a port. The presenter supported the concept of the trade, in concert with federal agencies such as Customs and the Coast Guard, defining minimum levels of security that seaports and seaport users could adopt as part of a cooperative initiative.

Two presenters felt that controlling the access of vehicles, and unauthorized personnel, to seaports and vessels was an

important issue. One presenter stated that the most critical components of security systems were adequate perimeter fencing and a means (identification cards for example) of controlling access to seaports. Another presenter stated that better controls could be achieved through the use of enhanced perimeter controls, identification cards, and the use of lists of personnel who are approved to be in seaports.

Some members of the trade expressed their views that security, and anti-crime initiatives, could be enhanced at seaports and facilities within seaports through the use of technology. There was some concern, though, that technology for seaports could be "over-engineered" (that is, there is a tendency for law enforcement agencies and the trade to attempt to develop and implement systems that will detect all types of crimes in seaports, although in most users' experience, this goal is unrealistic).

The role of the federal government in seaports was discussed extensively. One presenter stated that the federal government's role in addressing cargo thefts should be to review current regulations to ensure that companies are fairly compensated for their losses, enact laws to address cargo thefts, enact stricter guidelines for cargo theft convictions, and develop law enforcement task forces to address cargo crimes. Another presenter felt that the federal government needed to develop "partnerships" with the trade community to identify and address issues of related to crime and security in seaports.

In summation, the trade and members of the public who attended the session in Houston were concerned about crime in U.S. seaports. They believe that the theft of cargo at seaports is a major issue that can be addressed by the creation of a uniform database on losses and by ensuring that companies are fairly compensated for their losses. Enacting laws to address cargo thefts, setting stricter guidelines for cargo theft convictions, and developing law enforcement task forces to address cargo crimes were also identified as solutions to address the issues of cargo thefts. The trade also voiced support for restricting access to seaports through the use of identification cards, developing and adopting security guidelines that ports could follow, and identifying and placing technology at seaports to detect crimes.

Appendix E: Technology

The table at the bottom of the page indicates how technology associated with security, surveillance, and contraband detection relates to the major issue areas of the Commission.

The following sections provide a brief overview and comparison of the types of devices and systems expected to be commercially available within the next five years in each of the three technology categories covered in this appendix. The intent is to provide a realistic indication of the opportunities and improvements that could be realized by a focused and significant investment in seaport technology over the next several years.

Security Technology

Available Technology

Physical security and access control. The function of a physical security and access control system, or perimeter security system, is to deter, detect, document, and deny or delay any entry of the protected area. The most obvious seaport boundary to be protected by a perimeter security system is the external property line. In addition, physical boundaries need to be established for selected areas within the port. Often overlooked is the need for a security perimeter alongside cargo and cruise ships and along the water boundaries of the port, both at the immediate waterside and in the waterways approaching the port.

Fences can be used to establish and protect sensitive areas within the port such as the federal inspection area, the security office, high-value storage, lading and unlading areas next to ships, and the holding areas for mobile inspection systems. Protected zones can be established by a variety of commercially available electronic fences and physical barriers. Electronic line and area sensors also can be used to establish a temporary security perimeter around high-risk vessels or suspect containers. External intrusion sensors to meet every need are available from commercial or military sources.

Interior spaces can be protected by other types of sensors to detect entry into an area, movement within the area, or access to a sensitive item. They could be employed in office, equipment, and warehouse spaces as a backup to the perimeter sensors. Interior sensors might be used without external perimeter sensors only if the security response would be quick enough to respond

Issues Addressed by Technology Category

Issue	Security	Surveillance	Contraband detection
Prevention and detection of terrorism	X	X	X
Prevention and detection of crime	X	X	X
Military mobilization	X		X
Cargo control	X	X	X
Passenger and crew control	X	X	X

to the break-in before the thief could reach the target and flee the scene.

Gates and access controls must provide the same level of security as the fences and intrusion sensors. Personal ID cards or badges should identify both the person and the areas to which he/she is authorized access. Electronic codes embedded in the ID can be used both to verify authorized access and to record and track personnel movements for later analysis as needed. Electronic IDs or tags also can be applied to vehicles operating within port boundaries to control access and record movement. The IDs could be permanently associated with a vehicle or they could be attached to a truck and trailer when it enters the port and removed by the exit control guard when it leaves. The increased use of electric tags on commercial trucks offers another opportunity for identifying vehicles when they enter and leave the port and tracking their movement within the port. Gates that are dependent on a guard to control entry/exit must also be equipped with a means of preventing their use when the guard is distracted or absent.

A variety of biometric technologies for access control are already on the market or under commercial development. They can be used to control access to a physical area or to a particular item such as a computer or vehicle. The specific biometric could be a person's fingerprint, handprint, facial image, iris or retina image, voice, handwriting, or thermal image. Each biometric usually has an associated cost, benefit, and drawback that must be considered as a specific installation is planned. At present, the least costly biometric technologies employ facial image, single fingerprint, and either voice or signature recognition. Unfortunately, these inexpensive technologies also are subject to delay or defeat as a result of external factors such as lighting, cuts, dirt, background noise, or immature design. The most accurate and reliable technologies are the most expensive, possibly as much as 50 times the cost of the less expensive devices. As a result, each biometric technology should be individually tested on site.

In addition to ID access controls at pedestrian and vehicle gates, there are a number of portal control technologies to address general or specific threats. These include:

- Magnetometers to detect firearms, knives, or unauthorized tools.
- Radiation detectors for nuclear weapons or hazardous materials.
- Trace detectors to detect drug or explosive residue on clothing, hands, lunchboxes, door handles, steering wheel, car trunks, and so forth (see Contraband Detection Technology section below).
- Document scanners looking for drug or explosive traces on entry passes and ID documents; these and the trace detectors would help to detect not only smugglers but also drug users who might be a safety risk within the port.
- X-ray systems to scan packages (Figure 1), small items (Figure 2), or persons.

These security control measures at vehicle entry and exit gates can be enhanced on either a permanent or a random basis by employing some of the new mobile or relocatable X-ray and gamma-imaging systems capable of scanning an entire truck, container, or car for drugs, explosives, and other contraband. Additional information on these systems is provided in the Contraband Detection Technology section.

It would be preferable for security purposes that privately owned vehicles not be allowed within the security boundaries of the port at any time. Access by commercial vehicles should be limited to the areas for which they are authorized. Tire shredders and pneumatic/hydraulic bollards can be used to prevent the improper use of vehicle gates. License plate readers or electronic tags can be used to control and record the movement of commercial and private vehi-

cles, and weigh-in-motion sensors might be used to detect unusual loads or weight distribution in vehicles.

Adequate lighting throughout the port is another security necessity. Lights should be automatically controlled with an alarm to indicate any that are not operating. They should be sufficient to light all areas of the port, including the adjacent water. They also should be placed to prevent the creation of shadow areas if containers are stacked unusually high.

Closed-circuit television systems are a traditional means of providing perimeter and internal security, but their installation at seaports presents unusual problems. Like lights, they should be placed where they provide full and overlapping coverage of the fence, container, warehouse, office, and waterside areas. Cameras should have day and night capabilities and use motion sensors or alarm zones to home in on suspect activity. To avoid sabotage, power and signal cables should be hardened, and cameras should be programmed to automatically look at any camera installation that suddenly goes out of service. New advances in cameras providing a full 360-degree panoramic view should be explored. Infrared sensors could be used to complement the closed-circuit television systems, although they are less effective in moist air and fog. Long-range cameras mounted off port property often can provide surveillance of waterside activities, including gangways and the side of a ship away from the pier. The design of the closed-circuit television display room is as important as the camera installations themselves. Operators should not have to stare at multiple screens waiting for something to happen; the system should automatically alert them to actions of interest. Recording should be automatic to provide records for subsequent investigations.

Underwater sonar and passive sensors can be used to detect materials thrown into the water from a pier or ship regardless of whether the materials are packaged to float or to sink to the bottom for later retrieval. Electronic sensors also can be used to detect surface and underwater movement approaching the ships or piers, including small quiet boats and underwater swimmers. Side-scan sonar can be used to check vessels for external compartments that might contain contraband; the Customs Service has deployed both fixed and towed sonar arrays for this purpose. Finally, systems such as the Coast Guard's Vessel Tracking System can be used to monitor the movement of ships approaching and departing the seaport. That system can be augmented by one or more appropriately sited marine radars to detect and monitor small boat traffic around the seaport; the radars can in turn be supported by remotely controlled closed-circuit television cameras to provide visual records of suspect boats and their occupants.

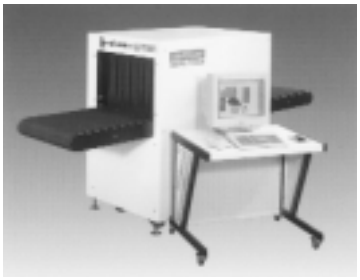


Figure 1. Parcel X-Ray

Protected voice and data communications within the port boundaries are another component of physical security and access control. Federal inspectors and agents need to communicate suspicious activity, check databases, access merchandise processing information systems, and coordinate their activities. Security officers and port operators also need to communicate their observations, check databases, and coordinate activities. Reliable seaport communications can be hampered by the widely dispersed areas of activity, the canyons created by stacked containers, and the difficulty in communicating aboard vessels and below decks. Radio repeaters may be needed on towers to improve system reliability; all voice and data transmissions should be in a protected or secure mode to prevent eavesdropping and jamming.

Figure 2. Portable X-Ray

Cargo security. The fences, lighting, closed-circuit television, access controls, and other perimeter security measures

described above will help prevent unauthorized access to containers and stored cargo. If a criminal does reach containers and cargo, security measures at the vehicle and pedestrian gates, at ship lading areas and gangways, and at waterside will make it difficult for stolen or smuggled goods to leave the port.

Inspection systems that permit the rapid nonintrusive examination of containers as they are unladed will reduce the opportunities for internal conspiracies and the removal of contraband before the container reaches the usual inspection site. These systems also will reduce the need to physically escort suspect containers from the pier to the federal inspection area. Appropriate systems are described in the Contraband Detection Technology section.

Additional cargo security enhancements include placing tamper-proof seals on containers and trucks, using container tracking technology to monitor containers, use micro-encapsulated taggants to reveal when containers have been approached or breached, and the use of information technology systems to integrate data used by both the public and private sector within seaports.

Passenger and crew security. Cruise ships transporting thousands of passengers represent both a potential means of transporting contraband and a potential terrorist target. Seaport security measures must ensure that passengers, crew, baggage, or ships stores are not used to get explosives and other dangerous materials aboard such ships or any other vessel, or used as a means of getting prohibited materials off of ships when they return to U.S. ports. Technology is available to identify passengers and crew with a high likelihood of having handled drugs, explosives, or firearms; to examine passengers and crew for internal and external body carries; and to examine baggage, stores, and equipment for concealed contraband. The smaller and less-expensive devices and equipment are suitable for being carried on a ship for use at intermediate ports of call; the larger, more expensive, and higher-throughput inspection devices may be feasible only at the port of embarkation. The applicable technologies include:

- Drug and explosive particle and vapor trace detectors.
- Drug and explosive wipes and sprays.
- Portable contraband detection systems, including dielectrometers and magnetic resonance for drugs and explosives in liquid form.
- Low-dose full-body X-ray.
- Medical X-ray.
- Ultrasonic and video scanners for liquid-filled drums and tanks.
- Baggage and parcel X-ray systems, including the computed tomographic (CT) X-ray systems used for airport baggage.
- Mobile X-ray and gamma-imaging systems.
- Trace detection using saliva, perspiration, or urine testing.
- Canines.

Access control and ID systems can be used to ensure that unauthorized persons leave a ship before it sails, and that all passengers return to a ship before it leaves a port of call. Bag match systems similar to those used at airports can guard against the introduction of terrorist devices or other unauthorized materials.

Military mobilization security. Using a seaport for a military mobilization greatly increases the security stakes. An act of terrorism or sabotage certainly can harm our overseas national defense actions, but in light of the munitions and other potentially dangerous materials that would be present, it also harms persons at the port and in surrounding areas. As the threat increases, the only way to control the risk is to reduce

vulnerability (risk equals threat times vulnerability). This means increasing the level of security and control throughout the port. It may be necessary to increase security rather quickly. The need for rapid security improvement can be offset to some degree if military assets can be used in addition to commercially available security technology, especially if the military assets are already in place.

The exact requirement for additional technology to raise security levels at a seaport will of course depend on the technology and the security level already in place. For example, if the existing perimeter fences are adequate but there is no protected buffer zone to prevent access to the fences, then the military can install ground and area sensors from its standard suite of unattended ground sensors. These sensors also can be used to quickly establish protected zones within the port. If the closed-circuit television coverage of the port is not sufficient to prevent and detect unauthorized movement, then military unmanned remote pilotless vehicles equipped with closed-circuit television and infrared sensors can be put in orbit over the seaport and its surroundings for 24-hour surveillance. A small tethered aerostat with a downward-looking radar launched from within 10 or 20 miles of the port would also provide continuous surveillance of vessel and vehicle traffic in and around the port in the absence of a Vessel Tracking System or ground-based marine radar.

A heightened level of security would justify using technology that might be considered too time-consuming or intrusive to protect normal commercial traffic and cargo. This might be as simple as increasing the quantity of nonintrusive contraband detection technology to permit more containers, trucks, cars, and people to be physically examined as they enter and leave the port. It might mean adding fingerprint and facial recognition technologies linked to automated databases of terrorist and criminal identifications. Or it might mean using security and contraband detection technologies with high probabilities of detection but with false alarm rates deemed too high for ordinary use.

Military mobilization conditions at a seaport would also mean more concern over the introduction of a weapon of mass destruction for activation in the port, while ships were in transit, or even after the military materiel was unladed at its destination. The portal and personal radiation detectors and isotope identification systems described earlier in this section and under Contraband Detection Technology would provide useful barriers against the introduction of nuclear material, but there is still little that can be done against the introduction of timed-release chemical and biological agents. A biological weapon can be as simple as a small aerosol can containing a liquid or powder, very difficult to distinguish from a spray lubricant or other innocuous item. A biological or chemical weapon also could be a fragile container designed to be crushed when a vehicle is unladed. Such small items are not likely to be detected by today's counterdrug or antiterrorism inspection technologies; even if detected they are not likely to be recognized as dangerous by the technology operator unless they were very much out of place. At this time, the best defense against such weapons is to limit access to as few persons as possible, to ensure that those few persons are a low risk, and to conduct frequent and thorough physical inspections. Should a remote prerelease trace detector for biological or chemical agents become available, it could be deployed at key locations around the port or operated from a low-flying remote pilotless vehicle.

Technology Under Development

Security technology is constantly being improved, driven by both private sector and government requirements for the increased protection of vital assets. As a result, we can expect to see considerable improve-

ment in system performance, especially in signal processing, and in unit cost.

Specific near-term improvements will include biometric technologies, including systems offering comparison of more than one biometric for each individual; improved facial recognition algorithms and database capabilities, including practical face-in-the-crowd systems; trace detection techniques using saliva and sweat analysis to detect internal body carries of drugs; more sensitive vapor trace detectors for drugs and explosives, enabling reliable screening of larger volume containers and spaces; and sensors to detect chemical and/or biological agent contamination on the outside of shipping containers. Electronic tagging and tracking systems for commercial trucks, railcars, and marine containers will be widely adopted by industry, making it easier to track these conveyances when approaching or within the seaport. Efforts spearheaded by the Australian Customs Service to develop a universal standardized system for reading and recording container IDs as they are being off-laded from ships may also be successful within the next five years. Commercial satellite systems providing high-resolution sea and land-surface images on demand are starting to become available, and competition should make accessibility affordable and easy.

Comparison of Security Technologies

Cost-benefit analyses for security technologies have some of the same pitfalls as for other types of law enforcement systems. For example, the security systems installed by the port operator are intended to prevent crimes such as cargo theft and drug smuggling, but the primary beneficiaries of such prevention are the shippers, consumers, and the public—that is, the entity incurring the costs receives little of the economic benefit. It is also difficult to measure the benefit of an event that does not happen—that is, the benefit of deterrence. The cost-benefit analysis can cope with this problem by looking at changes in crime over time and attributing the changes to the security technology added over that period, but it must also account for exogenous changes over the same period having nothing to do with the security technology. Finally, there can be tremendous disparities between the small cost of a single security component and the very large dollar value of the crime that was prevented by having that component in service.

The most likely approach to a cost-benefit analysis of security technology is to make it an incremental analysis—to look at the most likely added benefit of each increment of technology over the benchmark of the existing security system. In doing this analysis, it is essential to include the initial and recurring costs of acquiring and training the personnel who will be operating the security technology; ignoring this cost and the actual training activity means that the technology will soon fall into disrepair.

Any cost-benefit analysis of security technology is very dependent on the particular circumstances of each seaport, and a general quantitative analysis should not be attempted. However, several qualitative comparisons can be made as a guide to future technology choices.

- The most important technology components are the fences and gates for the perimeter of the port and high-risk interior areas. An automated ID access control system at all gates is preferable; at the minimum, a manual access control system can be handled by security guards if the system uses badges with the holder's picture and an indication of the areas to which he/she has access.
- The next requirement is adequate lighting and video coverage for all areas of the port, with a central control and monitoring facility.
- Reliable and protected communications are the third requirement.

- Nonintrusive inspection technology should be provided as soon as funding and staffing permit. Smaller, inexpensive units, including radiation sensors, hand-held contraband detection devices, and small X-ray systems should be part of the immediate equipment inventory. This technology should be augmented by mobile and relocatable X-ray and gamma-imaging systems phased into port operations as soon as possible, with the total number of systems depending on the vulnerability, criticality, workload, and physical layout of the port.

Surveillance/Monitoring Technology

Available Technology

Most of the technology required to investigate crimes in or involving seaports is the same as that required to investigate any type of crime anywhere. Obtaining this technology investigate seaport crimes is more a matter of priorities and resources than of new technology breakthroughs.

New technology that is more specific to the seaport environment includes covert or drop-and-run audio and video units to surveil suspect activities or containers. These units need to be concealed in the types of items normally found in the seaport environment. Preinstalled repeaters may be needed to ensure good communications from wherever the units are placed back to the monitoring point. Electro-optic systems must be adaptable to the contrasting lighting conditions of the seaport, from bright worklights to deep shadows in a single scene.

Smugglers will often relocate a container several times within the yard if they believe it is the object of surveillance; agents need covert radio frequency tags that can be quickly affixed to such containers so that their location can be tracked. Passive miniaturized microwave tags that can be concealed in high-value items or drug loads and detected if someone attempts to take the item through an exit gate are useful for theft and smuggling investigations.

Intrusion sensors can be built into gangways to alert monitoring personnel to attempts to board or leave a ship outside of normal access hours. Radiation sensors also can be built into the gangway or incorporated in mats at the foot of the gangway to detect the movement of radioactive materials.

First responders for a weapons of mass destruction alert or a hazardous material spill need information about the layout of the port or perhaps of a particular ship, as well as the nature of the hazard, likely contamination zones, and appropriate containment actions. Information on many hazardous spill situations is already available on small hand-held data units such as the Palmtop Emergency Action for Chemicals, and some is available in computer databases such as REACT that are readily accessible by subscribers to the service. Computerized layouts of the port that note hazardous material locations, sensitive building sites, emergency supplies, water hydrants, and other pertinent information for first responders can be loaded onto computer databases, provided to emergency response teams, and updated as situations change. Plans and drawings for cargo ships can also be put into a database. First responders also may need protective clothing and special material-handling equipment that is positioned close to entry points and readily accessible in emergencies.

Special technology can detect and record the evidence of environmental crimes such as the dumping of oil, hazardous waste, toxic substances, and other pollutants from ships moored in the port or underway. Airborne infrared sensors can detect many of these spills even if they are not visible to the naked eye; they also

can track the spill back to the vessel and provide documentation of the crime. Sensitive multispectral sensors developed for defense and intelligence requirements may provide even greater capabilities, including the opportunity for remote sensing. Small, relatively inexpensive sensor-equipped remote pilotless vehicles can perform aerial surveillance of suspect vessels or areas where spills often occur.

Technology Under Development

Improvements in these technologies can be expected over the next several years, particularly with respect to the availability of new sensors to detect environmental crimes. Incremental improvements in the surveillance, monitoring, and tracking equipment will also occur as data and signal processing capabilities improve and become less expensive.

Comparison of Surveillance/Monitoring Technologies

Investigative technologies are not very expensive, especially when compared with large-scale contraband detection systems or the fencing and access controls necessary to protect an entire seaport. In many cases it is difficult to predict in advance exactly what monitoring equipment or type of sensor will be needed for an immediate investigation. Therefore, it is prudent to acquire a reasonable inventory of equipment in advance based on experience and judgment about the number and types of investigations that may need to be conducted. Information technology and protective equipment for emergency response teams is also not very expensive, particularly in light of the lives and property that might be saved, and it should be a priority for acquisition at every seaport. The cost of environmental contamination along our waterfront and beaches can also be very high. The cost of acquiring and operating suitable monitoring equipment should not be very high by comparison. Such equipment not only can help pinpoint the offender, who may be subject to fines, but also can provide early warning of a spill so that preventive measures can be initiated immediately.

Contraband Detection Technology

These new contraband detection technologies, also called nonintrusive inspection technologies, use different approaches from the physical and chemical sciences and several packaging configurations to provide a variety of systems and devices addressing specific requirements. While a full discussion of the possible technology variations is beyond the scope of this report, the most significant characteristics and distinctions are these:

- **Substance-specific** or **anomaly detector:** Able to detect and identify a specific target substance, or able only to indicate something abnormal about the item being examined.
- **Trace detector** or **bulk detector:** Able to detect minute particles or vapors, or able only to detect larger quantities. Most trace detection devices are substance-specific; a bulk detector can be either substance-specific or an anomaly detector.
- **Imaging** or **nonimaging:** Provides a visual depiction of the item being examined, or provides a graphical display or signal (e.g., a red or green light). Trace detectors are usually nonimaging. Bulk detectors can be either, and sometimes provide both an image and a signal.
- **Portable**, **mobile**, **relocatable**, or **fixed:** A portable system can be easily carried or moved from place to place, either while in use or between uses. A mobile system may be in its own vehicle or on a towed trailer. A relocatable system can be disassembled and reinstalled at a new location in a few hours or days. A fixed

system is essentially limited to a single permanent location.

Each type of inspection technology will have its own set of operational characteristics, such as examination speed or throughput rate, probabilities of an accurate detection or of a false alarm, cost, maintainability, ease of operation, and safety. While the bad news may be that there is no silver bullet technology that will solve all seaport detection needs, the good news is that there are an increasing number of technology choices designed to meet one or more of those needs in an optimum fashion. The "correct" choice for each situation will be the best match of the technology's capabilities and characteristics with the intended operational application and requirements.

The choices can also be improved by combining different technologies in a single examination system—for example, combining a technology that is substance-specific with another that is an anomaly detector, or with technologies specific for different targets. One current example using both types of combinations is the mobile system that combines X-ray imaging, a drug and explosives trace detector, and a radiation sensor. As a result, an item can be examined quickly and reliably in one pass through the system for substances as diverse as drugs, guns, knives, explosives, munitions, radioactive weapons and waste materials, currency, and any other suspect materials whose presence might be indicated by an unusual shape or density.

Available Technology

Portable systems. Portable and hand-held inspection devices have long been the mainstays of the inspection process, particularly when looking for concealed drugs, explosives, and weapons. The list of popular devices includes gamma backscatter units, fiber optic scopes, laser and sonic rangefinders, trace particle and vapor detectors, flashlights and mirrors, steel probes and needles, chemical reagent sprays and wipes, and pager-sized radiation detectors.

Figure 3. Contraband Detection Kit

Figure 3 depicts a Customs contraband detection kit, which is a suitcase containing a gamma backscatter unit, fiber optic scope, rangefinder, detection sprays, segmented steel probe, needle probes, undercarriage or ceiling mirror, and flashlight. The kit, which is commercially available, provides the basic tools to search for concealments in the structure of a container, truck, or car, in baggage, and in small parcels.

Several systems are commercially available to detect trace levels of drug and explosive particles or vapor. The particle trace detectors are about the size of a desktop computer; the sampling device is carried to the suspect item, wiped over the surface, and then returned to the unit for analysis. The devices typically provide a "go/no go" signal and identify the item detected in 5 to 10 seconds. Units like these are in frequent use by the Coast Guard, the Customs Service, and Revenue Canada to check for traces of drugs on cargo and cruise ships, particularly in the crew's quarters, around popular hiding places, and on ship and crew papers. The vapor detectors are more widely used detecting explosives than drugs; they are easily carried, and they provide specific identification of the detected explosive within 5 to 10 seconds.

Particle detectors are also being used to detect drugs or explosives concealed within containers, vehicles, and baggage. Their accuracy of detection in such cases often depends on whether exterior surfaces have been contaminated by minute traces of the concealed substances, and they usually require physical contact with the surfaces being checked. However, current research in sampling techniques indicates that there may be ways around these limitations for the examination of closed marine containers and trucks.

New types of hand-held devices can detect the radiation emitted by nuclear weapons of mass destruction or other radioactive materials. One devise is a pager-sized radiation detector developed by a Department of Energy National Laboratory for the Customs Service. The device is extremely sensitive and will detect gamma radiation at levels only 2 to 4 times normal background and, depending on the radiation intensity, at distances up to 30 feet away. The isotopes detected include U-238, U-235, U-233, Pu-239, Pd-103, Co-60, Ces-137, K-40, and many others. The unit is worn on the inspector's belt and provides an automatic alert if radiation is detected. Customs is using more than 3,000 of these units at ports around the country.

Although the radiation pager is sensitive to a wide spectrum of radiation, it cannot identify a specific isotope. The radiation source could be as innocent as a medical implant or as dangerous as an improperly shielded commercial shipment or a terrorist device. While the specific situation usually will provide clues as to the correct interpretation, another device is needed to identify the specific nuclear material. One such commercially available device weighs about two pounds, stores the spectra of more than 250 isotopes, and will quickly provide the operator with exact information on the detected isotope(s), count rate, and other data. In practice, the two units complement each other, with the pagers providing continuous monitoring wherever personnel are working and the isotope identifier used when a radiation source is detected. The equipment inventory at a port could include a large number of the relatively inexpensive pagers backed up by just a few of the isotope identifiers. Together, the units provide an effective, affordable, and user-friendly nuclear detection capability for purposes of antismuggling, regulatory compliance, hazardous waste evaluation, and emergency response.

Figure 4. Mobile X-Ray Van

Mobile systems. The availability of mobile inspection technologies for seaport applications has improved considerably in the past year. Until then, mobile inspection technology was limited to relatively low-power and limited-capacity X-ray units mounted in small vans or trucks. These were essentially the same type of X-ray units used to examine baggage and parcels at airports and building entrances, with X-ray energy levels typically about 150,000 electron-volts (150 keV) or less. While the ability to move the X-ray equipment between loading docks was useful, the systems were limited to breakbulk cargo, which meant that containers had to be emptied and most pallets broken down to individual boxes. Figure 4 illustrates one of these mobile X-ray vans. The Customs Service has recently begun to equip its version of a mobile X-ray van with a particle drug and explosive detector as well as a radiation detector. Although the capacity is still limited to the equivalent of large packages, they can be checked for a variety of materials with one pass through the van.

Figure 5 illustrates the first in a new series of mobile inspection systems with higher energy levels than prior systems. Developed for Customs by the Department of Defense, this system was designed to inspect trucks and cars at land border crossings and is still being evaluated for use at seaports. In operation, the system moves along a line of stationary vehicles or containers using a 450-keV X-ray system to capture transmission and backscatter images of the targets in real time. It requires about 70 seconds to scan a 20-foot container, although under some circumstances, both sides of the container must be scanned, doubling the time. The average throughput rate is expected to be 7 to 15 vehicles or containers per hour. Based on experience with similar systems at land ports, this system should do well at imag-

ing most drugs, explosives, and other contraband that are hidden in the structure of containers, trucks, and cars or within relatively light cargo.

Figures 6 and 7 illustrate the most recent mobile inspection technologies for seaport applications. Although neither system had been deployed to a seaport as of October 1999, Customs and other agencies have done some evaluations that permit reasonable assessments of expected performance.

The system in Figure 6 uses gamma radiation rather than X-rays as the basis of its imaging capability. Like the mobile truck X-ray, the system moves along a row of stationary containers or vehicles and produces a real-time image very similar to that of an X-ray system. The cesium-137 source generates a beam energy of 662 keV, which approximates the penetration capability of a 1 MeV (million electric volt) X-ray source against typical targets. The scan time for one side of a 20-foot container is about three to four seconds, but again, both sides may sometimes need to be scanned. Based on its operational experience with a similar relocatable system at Port Everglades, Customs expects this system to perform well in examining trucks and containers loaded with light- to moderate-density cargo. Like the mobile truck X-ray, the system presents no radiation hazards to operators, bystanders, or the items being examined when it is operated in accordance with normal procedures, including personnel exclusion areas. The vendor claims that the system also can be used to examine a moving vehicle by ensuring that the cesium source is closed as the truck cab and driver pass through the inspection portal.

The system shown in Figure 7 was designed specifically to examine marine containers in a seaport environment. It features a high-energy X-ray system built into a container straddle carrier that can move under its own power between piers or examination sites; it provides a real-time scan as it is driven over a row of stationary targets. The X-ray system can be operated at 2,000 or 6,000 keV (i.e., 2 meV or 6 MeV), and it can examine full-height trucks, roll-on/roll-off units, single marine containers, or the upper container in a double stack. The scan time for a container is expected to be about 15 seconds. The 2 MeV energy level should be sufficient to examine all but the densest of cargoes, and the 6 MeV level should take care of most of those, including liquid-filled tanks. One drawback is that the system may not see the full height of an International Standards Organization container in a single scan. Customs expects to begin its operational evaluation of the first system at a South Florida seaport early in 2000.

Figure 5. Mobile Truck X-Ray

Figure 6. Mobile Gamma-Imaging System

Relocatable systems. A relocatable inspection system cannot move between inspection sites under its own power, but it can be disassembled and reassembled for operation at a new location within a few days. Systems that require several weeks to disassemble and reassemble are sometimes called “transportable,” but for this report they are considered fixed systems.

Only two relocatable inspection sys-

Figure 7. Mobile Container X-Ray System

tems are believed to be in use at seaports anywhere in the world. The system depicted in Figure 8 is said to be operational at a seaport in South Africa, and the system in Figure 9 is being operated by Customs at Port Everglades, Florida.

The system in Figure 8 is essentially a reconfiguration of an earlier dual-view 450-keV system developed to examine trucks on the Southwest border and later adapted to the single-view 450-keV mobile truck X-ray system illustrated in Figure 5. It requires that the target container or vehicle be towed between two 40-foot ISO containers that house two X-ray systems scanning each side of the target. Scan time for a 20-foot container is said to range between 45 and 180 seconds. Penetration capability should be better than in the mobile truck X-ray as a result of improved detector technology.

Figure 8. Relocatable Seaport X-Ray System

Figure 9. Relocatable Gamma-Imaging System

The system in Figure 9 is a different configuration of the mobile gamma-imaging system in Figure 6. In this case, the target vehicle or container is positioned between two parallel tracks on which the gamma source and the detector array move synchronously to create a scanned image. Scan time for a 20-foot container is under 30 seconds. This system also can be equipped with a cobalt-60 radioactive source, which increases the beam energy level to about 1.3 MeV and provides some increase in penetration and imaging capability over the cesium-137 version. The vendor is building for the Customs Service a stationary version of this gamma-imaging system to scan slow-moving railcars for hidden compartments, contraband, and persons. If that is successful, the same type of system could be used to scan railcars entering and leaving the seaport.

The Stolen Automobile Recovery System (STARS) is a gamma-imaging system demonstrated at a south Florida seaport to screen outbound containers for concealed stolen vehicles. STARS has the same cesium-137 source as the mobile and relocatable gamma-imaging systems described above, but it has a different set of detectors that decrease the imaging resolution so that only large items can be recognized. This change also reduces the cost of the system. During an operational evaluation at Port Everglades, STARS detected and identified vehicles in closed containers as they were driven into the port. Although not tested for other contraband detection applications or for vehicles leaving the port, it is possible that STARS could detect bulk quantities of drugs, weapons, or explosives being smuggled out of the port in a supposedly empty truck or container.

Fixed systems. A variety of fixed inspection systems are available for use at seaports. Figure 10 depicts a pallet examination system using two 450-keV X-ray systems, one scanning from the side and the other from the top. The system can handle pallets and cargo up to 4 feet wide, 6 feet high, and 10 feet long, and weighing 6,000 pounds. Although still using 450-keV X-ray systems, the side and top-down views provide a greater imaging capability than would a single-view system.

Several permanent facilities incorporate a high-energy X-ray system to examine trucks and marine containers. Systems operating at 8 to 10 MeV are being used in Europe and Asia, and 5-MeV systems are being used in England and France to scan trucks entering the EuroTunnel. At these energy levels the penetration and imaging capabilities are extremely good, but the facilities are quite large and expensive. The

scan time for a single container ranges from one to three minutes, but throughput can be increased with multiple inspection stations. Vendor claims for throughput are typically 20 to 35 containers per hour.

A prototype inspection system, built by a Department of Energy National Laboratory for the Customs Service, detects hazardous radioactive materials and bulk quantities of marijuana. This system detects potassium-40 (K-40) emissions that are several levels above background. Detectors below and on either side of the roadway automatically scan a truck as it approaches the exit gate of the port. By the time it arrives, the exit control officer knows whether there are radioactive materials in the truck and whether the source is likely to be a weapon, marijuana, or an industrial radiation isotope. The prototype system is still undergoing evaluation on the Southwest border; a relocatable K-40 detection system is also being tested on the Canadian border. If these prototypes are successful, they could fulfill both counterterrorism and counterdrug roles when installed at vehicle gates in a seaport.

Technology Under Development

Several of the technologies identified as available are in fact still undergoing prototype evaluation and are not in commercial production. However, there is already sufficient experience to permit high confidence in their becoming commercially available within the next 12 to 18 months.

In addition, there are several new inspection systems and enhancements to existing systems under development that may become commercially available and operationally viable within the next five years. Although some are only for smaller applications such as the examination of 55-gallon steel drums, or for specific targets such as drugs or explosives, most should have a more general application. Among the most likely and most significant potential improvements are these:

Figure 10. Dual-View Heavy Pallet 450 keV X-Ray System

- A 1-MeV X-ray system for cargo pallets and containers up to eight feet high and wide and weighing up to 10,000 pounds.
- Automatic alert to the probable presence of concealed drugs or explosives based on image interpretation.
- Central analysis and storage of container and truck images from remote inspection systems.
- A mobile STARS unit for detecting concealed vehicles and expected by the vendor to also be capable of detecting currency, high-tech exports, and other bulk materials concealed in empty or lightly loaded vehicles and containers.
- Application of the CT X-ray systems developed for fast, automated screening of air passenger baggage to the examination of the baggage and stores being laded aboard a passenger or cargo ship.
- Scaling-up of CT baggage systems to examine breakbulk cargo.
- Improved trace detection of drugs and explosives based on vapor.
- Micro-miniature electronic or biological sensors for the trace detection of drugs and explosives.
- Sensors to detect chemical or biological weapons or hazardous materials while in transit.
- Substance-specific detection systems to remotely examine containers and trucks using neutron analysis or other nuclear interrogation techniques.

However, as useful as some of these improvements and new products may be, their future availability does not justify delaying prudent investments in many of the systems currently available. In brief, there will always be a better technology just around the corner—but waiting until it appears can prevent any progress at all.

Comparison of Contraband Detection Technologies

This section provides an initial and somewhat qualitative basis for comparing the operational and economic value of available contraband detection technologies. A more detailed quantitative analysis would require information that is not readily available, such as the significance of the threat or of not detecting every smuggling attempt, the nature and quantity of the conveyances or materials to be examined, the actual performance of systems still being evaluated, and the true acquisition and life cycle costs of each system.

Even without information for a quantitative comparison of the various systems, some general guidelines and comments are possible as a guide to further investigation and decision making:

- The true detection performance of X-ray and gamma-imaging systems is a function of several factors, most notably the actual radiation energy level, the sensitivity and arrangement of detectors, and the signal processing and display characteristics. However, because it is easier to describe the energy level than the other parameters, that is the usual method for comparing systems. It is important to realize that changes in energy level and penetration level are not proportional. The table below is an approximation of the relationship between the energy level of the source and the number of inches of steel that the energy would penetrate.

  As a general rule, the sides, top, and floor of marine containers are built of heavier-gauge material than those of trucks. Marine containers also tend to be more tightly packed and to have heavier or more dense contents than truck cargoes. Therefore, the inspection of marine containers often requires greater penetration power than the inspection of trucks. While 450-keV units do well on most trucks, Customs expects that the examination of large, heavy cargo pallets will require an energy level of about 1 MeV, and that the thorough examination of most loaded marine containers will require 2 MeV or more.

- While the scan rate of an inspection system does have some influence on the overall throughput rate, the determining factors are more likely to be the time to move and prepare the containers or trucks that are to be examined and the time required to interpret the image. The time required to stage and remove vehicles depends on the space available to line them up; longer rows mean less time consumed in turning or reversing the system. The time needed to interpret the image also depends on many factors, but the Customs experience is 5 to 10 minutes for a large tractor-trailer combination or a loaded container. As a result, unless more image display stations are

X-Ray/Gamma Energy Levels and Approximate Penetration of Steel

Approximate Energy Level	Penetration (inches)
Less than 400 keV	Less than 1
400 to 700 keV	1.5 to 4
1 MeV	4.5 to 6
2 MeV	6 to 7
6 MeV	10
10 MeV	12

added, the sustained operational throughput rate of most imaging systems may be about the same regardless of differences in their individual scanning speed.

- Determining the real cost of the larger inspection systems must include consideration of the recurring costs of operation and maintenance. System reliability and the frequency and ease of maintenance should also be considered.

With these caveats in mind, some conclusions can be drawn about the relative value of the available systems.

Only three of the systems previously described were designed for seaport and marine container applications-the mobile 2- to 6-MeV system in Figure 7, the relocatable dual 450-keV system of Figure 8, and the fixed-site 8- to 10-MeV system. This is not surprising, since the impetus for the development of large new inspection systems was primarily the need to inspect the truck traffic crossing the U.S.-Mexico border. The table on the next page compares some of the salient features of each system. It is important to remember that no first-hand information exists on the operational performance of the mobile and relocatable systems; the former because the prototype system has not gone to the field, and the latter because information is not yet available from the South African operator of the system. Some system characteristics, such as the realistic sustainable throughput rate, can be determined only by operational experience.

Although the relocatable gamma-imaging system was initially envisioned for vehicle examination at landports, the Customs Service is using one at a seaport now and plans to add more at seaports over the next year. For this reason it is also included in the table below, based on the current configuration.

Examination systems that are smaller and less expensive than the specially designed marine container systems described in the table below can play a valuable role at seaports even though they provide lower energy levels and thus less penetrating power. Mobile systems can be used to screen trucks, containers, and cars at entry and exit gates. They also can be used to examine empty or lightly loaded containers within the container yard and to scan containers at the pier as soon as they are offladed. Relocatable systems can be used in either temporary or permanent installations to augment the overall examination capability of the seaport. Although there is not much experience or data thus far on the use of mobile truck X-ray systems in a seaport environment, Customs is successfully using the relocatable gamma-imaging system depicted in Figure 9 at Port Everglades against a variety of marine cargoes and containers. While X-ray systems have long been the traditional imaging tool for customs-type inspections, the new gamma-imaging systems have the potential for performance comparable to a higher-energy X-ray system but in a simpler, more reliable, and less expensive package.

The available CT X-ray systems are designed specifically to examine airline baggage and have not been tried in other environments. They are limited in the size of the objects they can examine, and they offer energy levels of 200 keV or less. However, their ability to create 3-D images of the target and to provide an automatic alarm for even very small quantities of suspect materials may be useful for the rapid screening of baggage and similar-sized stores being laded aboard a ship.

Inspection systems that are mobile or easily relocatable can be an essential component of military mobilization or emergency response plans. The mobile 450-keV X-ray and mobile/relocatable gamma-imaging systems described above can be quickly moved over the road or by rail; several versions can be easily airlifted. The mobile 2- and 6-MeV X-ray system

Comparison of Marine Container Systems

	Mobile 2 & 6 MeV	Relocatable Dual 450 KeV	Fixed 8 to 10 MeV	Relocatable Cesium 137
Estimated acq. Cost	$4M	$3M	$10–12M	$1M
Site/space req.	Minimal	Moderate	Extensive	Minimal
Penetration—inches	7 & 10	3	10–12	5–6
Transmission image	Yes	Yes	Yes	No
Backscatter image	No	Yes	No	No
Scan full-height	No	Yes	Yes	Yes
Scan double-stacked	Yes	No	No	No
Examine at pier	Yes	No	No	No

built into a straddle carrier can be moved between ports by barge. Operator training on all of these systems can be accomplished in a very short time, or a cadre of trained operators could be available for call-out.

Technology now available for the specific detection of nuclear, biological, and chemical weapons of mass destruction while in transit is limited to the detection of nuclear materials, primarily by the detection of gamma radiation. While the radiation detectors could be defeated by heavy shielding, the shielding itself should be detected by X-ray and gamma-imaging systems and recognized by inspectors or automatic detection systems unless it was designed to look like a normally dense commercial product. Fixed sensors to screen moving trucks and containers for radioactive materials at traffic chokepoints are commercially available with a range of selectivity and sensitivity. Radiation detectors also can be added to standard imaging systems; Customs is currently completing the installation of such detectors on all of its fixed and mobile X-ray systems for examining cargo and baggage. The small, inexpensive radiation detectors can extend radiation detection capability to every location visited by inspection personnel. Technology to detect chemical and biological weapons during transit (i.e., prerelease) is still under development; the applicability of vapor and particle trace detectors will depend in very large measure on the presence and detectability of external contamination of the container used to transport the agent. Unusual packaging to protect these weapons during transit may also be recognizable on imaging inspection systems.

Appendix F: Model Port

As noted in Chapter 5 and articulated in Recommendation 14 of the Commission's report, the proposed national-level security subcommittee should develop a "model port" and draft guidelines for its use by seaport stakeholders in reducing port security-related vulnerabilities. The subcommittee should then manage an associated outreach program to ensure that the model port is broadly disseminated and widely accepted. The reduction of vulnerabilities would, in turn, be an integral element of effective risk mitigation. The relationship between threats, vulnerabilities, and risk is discussed in detail in Chapter 5.

The model port guidelines should be sufficiently flexible to be applicable to all domestic ports, regardless of size, management, or type, and spectrum of potential threats. Local and national crime and terrorism threat assessments, along with national threat-warning information, are tools that should be used in conducting a vulnerability assessment at the port level. These assessments are included in recommendations 5 and 7 of the Commission's report. This vulnerability assessment is the primary tool by which risk should be determined at the seaport.

Stakeholder input to the subcommittee should be sought from such industry groups as the Maritime Security Council, the National Cargo Security Council, the International Association of Airport and Seaport Police, and the American Association of Port Authorities. Furthermore, security practices at ports throughout the world should be analyzed for potential "best practices" that can become guidelines.

Because U.S. seaports vary significantly in size, management scheme, trade, and types of threats, the model port should be flexible enough to fit all types of commercial ports at both normal operating conditions and heightened periods of risk, primarily as a result of increased threat and medium or high vulnerability. At a minimum, the following criteria should be incorporated into the desired attributes of a model port.

Physical Security and Access Control

Standard Operating Procedures

- A local port security committee is chartered, comprised of appropriate federal, state, and local agencies, as well as port stakeholders.
- The port has conducted, in conjunction with federal, state, and local law enforcement agencies, a crime threat assessment.
- The port has, through the port security committee, received information from the results of the terrorism threat and vulnerability assessments.
- The port authority or terminal operator provides a current security manual incorporating standard operating procedures, standards of conduct, and a definitive statement of what the management expects of the security force.
- The security manual is fully documented, complete, and accurate, and consistently adhered to.
- The security director formulates written operating procedures for security-related

matters, including bomb threats and alert levels, and collaborates with relevant government and law enforcement agencies to develop an emergency response plan.

- Adequate and reliable communications are provided to enable contact between elements of the terminal security force and from the security force to local law enforcement.
- Terminals handling a substantial volume of cargo or passengers to identify personnel authorized to enter cargo, passenger, and document processing areas employ an employee identification card system.
- Display of an employee identification card, visible at all times, is required of each employee.
- Supervisory personnel are present during lunch and breaks if taken in the work area.
- Truck drivers, vendors, and other visitors are not permitted in the general offices of any terminal other than as required to conduct their business, and only authorized personnel are permitted in warehouses.
- Computer security formal guidelines are in place for each marine terminal.
- Computerized information access is password-controlled, and is restricted on a need-to-know basis, which includes dissemination of information no sooner than required to complete transactions involving, for example, shipping agents.
- Firearms are restricted in the seaport to law enforcement personnel and other approved individuals.

Perimeter Fence Line

- Fence line is intact, taut, well-secured to upright supports anchored into the ground, topped with barbed wire on outward facing angle irons, and stands at least 8 feet (2.5 meters) in height.
- Reinforcement of the fence line with a barrier (e.g., ditch or berm) is used to enclose wheeled operations involving containers on chassis or trucks loaded with consolidated cargoes overnight, to render certain parts of the fence line physically impassible for a trailer.
- Alarms are installed to complement the security of a reinforced fence line to form a system capable of monitoring many alarm zones from a central control room manned by terminal security personnel.

Parking

- Parking areas are situated outside of fenced operational areas or a substantial distance from cargo handling and storage areas and buildings, and passenger embarkation areas.
- Employees exiting to the parking area from a cargo or passenger facility are required to pass through a controlled area under the supervision of security personnel.
- Employees visiting their motor vehicle during work shifts are required to notify management or security personnel.
- Control of access to employee parking areas is supervised, and is restricted by a permit system, with records maintained that include matching personnel with permit number and motor vehicle identification. Temporary permits are issued to vendors and visitors for parking in designated controlled areas.

Access Points

- Gates in disuse are permanently sealed or removed.
- Gates considered indispensable and in daily use are secured by two sets of padlocks and case-hardened steel chains, or

deadlocking bolt or an equivalent device, that does not require use of a chain.

- Gates are equipped with a recording system to document inspection stops by security personnel during routine patrols.
- Separate gates are constructed for the use of personnel and vehicular traffic, which include personnel screening points.
- Gate alarms are installed and monitored from a central point (e.g., main guard-house).
- Gatehouses at all vehicle entrances and exits are manned during business hours by operators of facilities handling a substantial volume of high value cargo, and are situated so that exiting vehicles may be halted and examined on terminal property, and are equipped with telephones or other communications devices.
- Closed circuit television systems are used for control of the interior and perimeter of the terminal; they record entry and exit through the main gate, and images of container and vehicular license or registration numbers. Drivers are stored for designated periods.
- Operational information obtained by terminals during the entry stage is made available to the security department for its purposes to, for example, ensure and verify that a particular container was released to a specific driver.

Lighting

- Controlled adequate lighting is provided to enable clear illumination for all facility areas, including perimeter fence lines, entrances, exits, and gatehouses, and sufficient to assure proper visibility of approaching persons and vehicles.
- The seaport authority ensures that all areas of the terminal are illuminated to at least the level of twilight, even when there is no activity. While in port, the ship's deck and hull is illuminated in periods of darkness and restricted visibility, but not so as to interfere with the required navigation lights and safe navigation.

Buildings

- In areas adjacent to warehouses, sheds, and passenger terminals, a buffer zone of at least 10 feet is created around the entire building and must be enforced at all times.
- Containers obstructing the view of building entrances by police and security guards are removed.
- All exterior doors and windows are equipped with properly installed locks or locking devices, and incorporated with detection or alarm systems.
- Area alarm systems are installed to secure computer rooms and office spaces where confidential documents are stored.
- A key control system is implemented, with a formal policy governing which personnel have right of access to specified areas. A master ledger is maintained recording the legitimate holder of each copy of each key, issuance for which is controlled by management or security personnel.
- Locks, locking devices, and key control systems are inspected regularly, and malfunctioning equipment is repaired or replaced.

Security Force Management

- The security director establishes minimum hiring standards, and ensures their compliance.
- Training is made imperative for in-house or contracted security force personnel, all of whom receive adequate pre-work classroom training and certification by

a qualified professional. The training includes completion of basic security topics, and at least 16 hours of on-the-job training. If national, state, or local standards or certification regimes are in place, training meets or exceeds those requirements.

- The security director's written job specifications include the task of maintaining and validating the published information in the security manual, and this is an assessment element in the manager's formal performance review.
- Security personnel frequently patrol terminals to ensure that gates, fence line, and buildings are secure.
- Security personnel are required to complete a work sheet during each shift, recording the duties performed by them and at the times of occurrence.

Enhanced Measures for Physical Security and Access Control in Periods of Heightened Risk

- All individuals employed in the seaport who have access to restricted or secure areas have been subject to background and criminal record checks.
- In addition to port facility employees, photo ID badges are displayed by vessel crewmembers, other carrier employees, vendors, longshoremen, passengers, and visitors to prevent unauthorized access to restricted areas.
- Intrusion Detection Systems including video monitoring, remote sensors and alarms, and computerized recording instrumentation are employed to facilitate real-time evaluation and response and subsequent investigation and analysis.

Cargo Security

Delivery of Cargo

- Gate passes are issued to truckers and other carriers to control and identify those authorized to pick up cargo.
- The company name of carriers is clearly shown on all equipment.
- Cargo is only released to the carrier specified in the delivery order unless a release authorizing delivery to another carrier is presented and verified.
- Personnel processing delivery orders verify the identity of the trucker and trucking company before releasing the shipment.
- Access to areas where documentation is processed is limited solely to authorized personnel, and shipping documents are safeguarded from theft.
- Seal numbers on containers are verified against documents, and seals are checked for integrity.
- The insides of conveyances are checked for stolen merchandise.
- Drivers sign for shipments legibly and in ink.

Reception of Cargo

- Drivers entering facilities with deliveries in all cases obtain gate passes.
- Drivers show identification, and the company name of carriers is clearly shown on all equipment.
- Delivery documents (such as bills of lading) are closely scrutinized, seal numbers on containers are verified against documents, and seals are checked for integrity.
- Cargo shipments should be verified upon receipt.

Security of Cargo During Lading and Unlading from Vessels and Railcars

- Cargo is moved directly from railcars or vessels to storage facilities, and directly from storage facilities to railcars and vessels.
- Seals are checked on all containerized shipments before arrival/departure/transfer.
- Empty containers are opened, examined, and resealed, and stored door-to-door in facilities.

Storage of Loose Cargo

- Cargo stored in open areas, and palletized or stacked cargo stored in warehouse facilities, are properly stacked and placed within, away from, and parallel to fences and walls, to ensure unimpeded views for security personnel.

Documentation Review and Control

- Ocean manifests for cargo to be unladed are transmitted electronically to Customs in advance of vessel arrival.
- Bills of lading for cargo and containers are checked for accuracy before acceptance.
- Cargo on documentation is adequately described, and the weights and piece counts indicated on documentation.
- Cargo documentation is closely guarded to avoid documentation fraud.

Cargo Control, Inventories, and Cargo Reconciliation

- Facility operators maintain, and continuously update, an accurate list (paper or electronic) of all cargo in facilities and a location chart of all cargo, and containers in their facilities.
- Import cargo, export cargo, and domestic cargoes are segregated.
- Delivery and receiving operations are segregated.
- Overages and shortages are reported immediately.

High Value Merchandise

- High value commodities are stored in cribs or security cages designed to resist forcible entry from all sides, and separate logs and procedures for the release and receipt of these commodities are maintained.
- High value merchandise in mounted containers is placed in a secure holding area where it can be observed by management or security personnel at all times, and separate logs and procedures for the release and receipt of these containers are maintained.
- High value cargo in containers is placed on the upper tiers of container stacks in order to limit their accessibility, and the containers are also stacked so that the doors of each container abut each other.

Seals and Sealing Practices

- Seals are inspected whenever a sealed containerized shipment enters or leaves a facility. If the seals are not intact, or there is evidence of tampering or the seals are not correct, security is notified and the cargo in the container is tallied.
- Unsealed containerized shipments are sealed at the point of entry to the facility and the seal number is noted on shipping documents.
- Seals are stored in a secure place, access to seals is restricted, and a log noting the distribution of seals is kept.
- Seals are also checked and their numbers, date, time, and place of examination recorded at each of the following times: arrival at/leaving the terminal gate, during stacking; relocation within the terminal; loading/discharge from a vessel; whenever the container doors are opened.

Equipment Control

- Access and keys to equipment such as yard mule tugmasters, trucks, or high loaders are strictly controlled.
- Equipment is kept in a secure and specified area when not in use.

Personnel Security

- Prospective employees are required to provide background information about previous employment history, criminal records, and drug use.
- All prospective employees are fingerprinted as part of the application process, and criminal history records are performed on all prospective employees (to the extent permitted by law).
- Employers have "drug awareness" and security education" programs in effect for all employees.
- Employees wear distinctive identification cards or badges that act as authorization for accessing restricted areas.

Audit Trails, Correcting Vulnerabilities, and Reviewing Procedures

- Procedures are in place that will permit investigators, when reviewing documentation, to determine how and when any cargo or containers were removed from an operator's custody in an unauthorized manner.
- When an operator's system is compromised, and cargo or containers are removed from an operator's custody in an unauthorized manner, procedures are in place to identify the deficient procedures/practices and corrective action is taken to ensure that a similar incident does not occur.
- Managers review procedures periodically to ensure that new threats and procedural vulnerabilities are identified as they arise.

Enhanced Measures for Cargo Security During Periods of Heightened Risk

- Seaports where foreign cargo arrives have a separate Federal Inspection Station. Access to these areas is limited solely those to that have previously received approval to enter the area.
- A closed circuit television system is used to record activities during lading and unlading procedures, and within cargo processing and trucking facilities.
- Port authorities, terminal operators, warehouse operators, and trucking companies have installed automated access control systems in order to monitor access to restricted areas.
- Port authorities, or terminal operators, employ non-intrusive technology (such as X-ray or gamma ray systems) to identify contraband and/or verify cargo shipments.
- Trucking companies use an automated system (such as Global Positioning Systems or cellular) to track trucks and shipments.
- Firms have developed and implemented "Integrated Security Concepts" into their operations to deter and prevent internal conspiracies from occurring.

Security of Passengers and Crew

- The introduction of prohibited weapons, incendiaries, or explosives aboard passenger vessels, on persons, within personal articles or baggage, or in stowed baggage, cargo, or stores is prevented or deterred.
- Passenger vessels throughout a voyage maintain a high level of gangway security. These security measures include some form of biometric identifier (such as a photograph), to prevent the unauthorized boarding and re-boarding of persons after port calls.

- Timely, accurate, and complete passenger and crew arrival and departure manifest information is submitted by carriers to the Immigration and Naturalization Service.
- All members of a passenger vessel's crew are adequately trained to perform their security-related duties.
- Physical and operational security measures are coordinated between passenger terminals and passenger vessels whenever a vessel is moored at the terminal.

Enhanced Measures for Passenger and Crew Security During Periods of Heightened Risk

- Seaports where international passengers arrive have a separate Federal Inspection Station. Access to these areas is limited only those to that have previously received approval to enter the area.
- Visitors/passengers gain access to a terminal facility through a designated screening point that should include a metal detector and X-ray system.
- Automated access control or magnetic stripe cards are utilized rather than keys to enter terminal facilities.
- The Advance Passenger Information System is utilized by carriers and is submitted in a timely fashion to Immigration and Customs so that law enforcement checks can be performed before a vessel's arrival in the United States.

Military Mobilization Security

- The local Port Readiness Committee actively meets and coordinates its effort with the local port security committee. All applicable federal, state, local, and commercial entities must be included in its membership.
- The Port Readiness Committee has a written and current memorandum of understanding.
- A Port Readiness Exercise has been conducted within the last two years.
- The local Port Readiness Committees actively participate in Defense Department-sponsored mobilization exercises/cargo movements in addition to their own exercises.
- The local Coast Guard Captain of the Port addresses security for military mobilization in his/her planning documents.

Enhanced Measures for Military Mobilization Security During Periods of Heightened Risk

- Any "lessons learned"/problems, as outlined in the latest Port Readiness Exercise Final Report, have been resolved or are in the process of being actively resolved.
- If a Department of Defense vulnerability assessment was done on this port, the vulnerabilities, if any, have been adequately addressed by the Port Readiness Committee.

In order to assist local governments and the commercial maritime industry in managing security risk, the model port should also employ recommendations or procedures that are applicable at varied risk levels in order to reduce specific or general vulnerabilities. The matrix on the next page is an example of the type of format that can be employed to show the flexible measures that can be taken in the face of variable threats and different types of ports. Details regarding the specific vulnerability reduction guidelines that populate the outline can be disseminated via media such as Transportation's *Port Security: A National Planning Guide* series.

Model Port Concept Outline

I. Intent: To provide 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.

II. Standards Matrix:

Focus Area	High Risk	Medium Risk	Low Risk
Standard Actions	■ Low and Medium Risk actions plus implement additional steps identified in Security Plan. ■ Conduct regular assessments. ■ Implement critical infrastructure protection measures.	■ Low Risk actions plus implement additional steps identified in Security Plan. ■ Conduct regular assessments.	■ Comply with applicable federal regulations. ■ Complete vulnerability and threat assessments. ■ Develop Security Plan. ■ Table top exercise. ■ Conduct periodic assessments. ■ Personnel awareness training. ■ International cooperation.
Crime Prevention	■ Enhanced Surveillance Systems. ■ Cargo tracking systems. ■ Increased coordination with law enforcement.	■ Security guards certificated to meet standards.	■ Credentialing. ■ Access control to terminal property. ■ Security guards from reputable company. ■ Video surveillance system.
Terrorism	■ Increased coordination with Joint Terrorism Task Force.	■ Increased number of guards patrolling. ■ Attend to gaps identified in vulnerability assessments.	■ Same as Crime Prevention steps.
Intelligence/ Information Security	■ Anti-hacking measures employed.	■ Outreach to maritime community regarding threats and preventive measures.	■ Links to local/state/federal law enforcement and federal government intelligence. ■ Password security.
Cargo Security	■ X-ray and other sensor scans of import and export cargo.	■ Increase targeting cargo shipments.	■ Cargo tracking systems.

Model Port Concept Outline (cont.)

Focus Area	High Risk	Medium Risk	Low Risk
Passenger and Crew Security	■ 100 percent screening of people and baggage.	■ At least 30 percent screening of people and baggage. ■ Biometric and photo ID.	■ Some screening of people and baggage. ■ Accurate, timely manifests.
Military Mobilization Security	■ Constant communications between agencies/facilities.	■ Updated planning. ■ Updated memorandum of understanding.	■ Port Readiness Committee meetings.
Inter-Agency Coordination	■ Live watch command center with agency representation.	■ Outreach to commercial facilities.	■ Regular meetings at port level.

Selecting Technology for a Model Seaport

Selecting the appropriate complement of security, surveillance, and contraband detection technology for a seaport requires a case-by-case analysis of the current security status of each port, the size of its physical facility and annual workload, geographic considerations, and other factors. Nonetheless, it is possible to arrive at three nominal levels of technology deployment based on arbitrary estimates of port requirements.

Minimal Low-Cost Implementation

At this level, we assume a relatively small seaport that is considered to have a low risk of criminal activity and is not designated as a military mobilization port. The goal is to bolster security at the port to the level at which most criminal activity is deterred, although the port would still be vulnerable to a dedicated exploitation by the criminal element.

The investment in physical security technology would be primarily for fences, lighting, and closed-circuit television, with no electronic or automated access controls. Perimeter buffer zones would be unsensored. The only interior security area would be the federal inspection facility. The investment in radio and data communications would be minimal; waterside security would be primarily by closed-circuit television and physical patrol. Approximate cost would be $2 million.

Cargo security and passenger/crew security would be accomplished with handheld/portable inspection technologies augmented by parcel X-ray systems, and by a badging system for persons boarding and leaving ships. Approximate cost would be $1 million.

Because military mobilization is not anticipated for this port, there is no technology requirement for this application. The investment in investigative, first-responder, and environmental crime technology would also be minimal. Investigative equipment would be limited to a small selection of the most frequently used equipment and devices and no pre-installed equipment; the investigative posture would be reactive rather than proactive. First-responder protective equipment and clothing investments would be small;

considerable dependence would be placed on outside fire and police resources to deal with any emergencies. Surveillance for environmental spills would be by periodic rental of a light aircraft with hand-held cameras and electro-optic equipment. Approximate cost would be $1 million.

Contraband detection technology would consist of one mobile 2- and 6-MeV X-ray system, three mobile or relocatable gamma-imaging systems, a mobile X-ray van, and a number of portable and handheld devices including particle and vapor trace detectors for drugs and explosives. Radiation sensors would be at vehicle and pedestrian gates but no other locations. Approximate cost would be $8 million.

Total estimated cost is $12 million, with a probable range of $10 to $15 million.

Mid-Range Implementation

This port requires a higher level of security because it handles shipping from politically sensitive foreign countries and/or large amounts of high-value commodities, because it is a potential military mobilization port, or because it has a high volume of cruise ship traffic. The goal is to actively deter and deny most criminal or terrorist activity and to have the port at a state of security preparation that could readily be increased to the maximum level if necessary.

The physical security investment would be increased to provide external and internal sensors protecting the federal inspection area, high-value storage areas, the security/closed-circuit television control room, and access to arriving or departing vessels. All gates would have electronic access controls; the interior security areas would incorporate biometric systems for added protection. Unattended ground sensors to detect movement near the exterior fences would protect buffer zones. Receiver systems would be added to receive electronic ID information from tagged trucks and containers. Radio repeaters would be installed to provide reliable voice communications. Waterside security would use closed-circuit television and towed sonar systems. Approximate cost would be $3.5 million.

Cargo security and passenger/crew security would be augmented with additional technology to detect explosives, firearms, drugs, and other contraband. Automated ID badges would be required for all crewmembers. All vehicles entering and leaving the port area would be inspected with a STARS-type system; these inspections would be randomly heightened by using a higher-energy mobile X-ray or gamma-imaging system. Approximate cost would be $3 million.

Technology for use in the event of a military mobilization would be staged at a military depot where it could be deployed to several different ports depending on the mobilization scenario. This technology would include waterside sensors to detect swimmers or packages dropped into the water, a remote pilotless vehicle system with air vehicles and control system, electronic sensors to establish additional security boundaries, and additional portal and personal radiation detectors. Approximate cost would be $0.5 million.

Investigative, first-responder, and environmental crime technology would be increased to allow a proactive investigative mode and significant interactions to prevent criminal activity. First-responder technology would include computerized information on the port and on actions to be taken in the event of chemical spills, improperly packaged hazardous materials, and other crises. Environmental technology would include an infrared system installed in a rented helicopter for regularly scheduled surveillance flights. Approximate cost would be $2 million.

The complement of contraband detection technology would be increased to add a second mobile 2- and 6-MeV container X-ray system, two more mobile or relocatable gamma-imaging systems, additional portable inspection systems including small and parcel X-ray units, radiation pagers for all inspection personnel, and a number of isotope identifiers. Approximate cost would be $15 million.

Total estimated cost is $24 million with a probable range of $18 million to $27 million.

Maximum-Level Implementation

At this level the intent is to reduce cargo theft, smuggling, and other criminal activity to a minimum in order to protect military assets and high-value cargo and to put maximum interdiction pressure on a major smuggling route. Sufficient technology would be employed to provide the necessary levels of enforcement and compliance measurement without impeding the movement of legitimate traffic.

The physical security investment in technology would add biometric sensors at all entry and exit points; electronic tracking of all vehicles moving within the port; and a full complement of waterside sensors including marine radars, closed circuit television, and fixed and towed sidescan sonars. Redundant voice and data communication links would be installed, and closed-circuit television cameras to surveil areas outside of the port for suspicious activity would be added. Approximate cost would be $7 million.

Cargo security and passenger crew security technology would be increased by additional systems to screen incoming and departing vehicle and pedestrian traffic and to screen all materials and baggage going aboard ship. Approximate cost would be $4 million.

Investigative technology would be increased, primarily for electro-optic and audio monitoring systems. Environmental technology would include a multisensor aerial or remote sensing surveillance system. Approximate cost would be $3 million.

Military mobilization technology would be deployed to the port to ensure routine nonintrusive inspection of all containers and trucks entering the staging area for military materiel. Sensor-equipped remote pilotless vehicles would be used to monitor the port and surrounding areas. Approximate cost would be $3 million.

Contraband detection technology would be increased by two more 2- to 6-MeV mobile X-ray systems, two more mobile gamma-imaging systems, a gamma-imaging system for rail traffic entering the port, and two mobile truck X-ray systems. Approximate cost would be $27 million.

Total estimated cost is $44 million, with a probable range of $38 million to $50 million.

Technology Summary

Keeping in mind that the cost of technology implementation for a specific port will depend on its individual characteristics, requirements, and existing capabilities, the estimated cost of the technology described above for the three nominal levels of implementation is summarized in the table below.

Estimated Cost of Technology By Implementation Level ($ Million)			
Application	**Minimum**	**Mid-Range**	**Maximum**
Physical security	2	3.5	7
Cargo, passenger, crew security	1	3	4
Military mobilization	—	0.5	3
Investigative, first responder, environmental crime	1	2	3
Contraband detection	8	15	27
Total	12	24	44
Probable range	10–15	18–27	38

State of Florida Seaport Security Study

Finally, the state of Florida's Office of Drug Control is sponsoring a broad, comprehensive assessment of security (and related issues) at the state's 14 deep-water ports. This objective assessment is to develop a viable plan to implement enhancements that solve drug interdiction, money laundering, and general port security problems. This plan is covered in Appendix C.

The State of Florida Seaport Security Study topics clearly have relevance to the work of the Commission, and the study presents an opportunity to prototype many of the items listed earlier in this appendix.