

April 2005

MARITIME SECURITY

New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-05-394](#), a report to congressional requestors.

Why GAO Did This Study

Sharing information with nonfederal officials is an important tool in federal efforts to secure the nation's ports against a potential terrorist attack. The Coast Guard has lead responsibility in coordinating maritime information sharing efforts. The Coast Guard has established area maritime security committees—forums that involve federal and nonfederal officials who identify and address risks in a port. The Coast Guard and other agencies have sought to further enhance information sharing and port security operations by establishing interagency operational centers—command centers that tie together the efforts of federal and nonfederal participants. GAO was asked to review the efforts to see what impact the committees and interagency operational centers have had on improving information sharing and to identify any barriers that have hindered information sharing.

What GAO Recommends

To help ensure that nonfederal officials receive security clearances in a more timely fashion, GAO recommends that the Coast Guard (1) develop formal procedures to use data as a tool to monitor the security clearance program and (2) raise the awareness of nonfederal officials about the process of applying for a clearance. The Department of Homeland Security and the Coast Guard concurred with our recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-05-394.

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

MARITIME SECURITY

New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention

What GAO Found

Area maritime security committees provide a structure that improves information sharing among port security stakeholders. At the four port locations GAO visited, federal and nonfederal stakeholders said that the newly formed committees were an improvement over previous information sharing efforts. The types of information shared included assessments of vulnerabilities at port locations and strategies the Coast Guard intends to use in protecting key infrastructure.

The three interagency operational centers established to date allow for even greater information sharing because the centers operate on a 24-hour-a-day basis, and they receive real-time information from data sources such as radars and sensors. The Coast Guard is planning to develop its own centers—called sector command centers—at up to 40 additional port locations to monitor information and to support its operations. The relationship between the interagency operational centers and the planned expansion of sector command centers remains to be determined.

The major barrier hindering information sharing has been the lack of federal security clearances for nonfederal members of committees or centers. By February 2005—or 4 months after the Coast Guard developed a list of 359 committee members who needed a security clearance—28 of the 359 members had submitted the necessary paperwork for a security clearance. Coast Guard field officials did not clearly understand that they were responsible for contacting nonfederal officials about the clearance process. To deal with this, in early April 2005, the Coast Guard issued guidance to field offices that clarified their role. In addition, the Coast Guard did not have formal procedures that called for the use of data to monitor application trends. Developing such procedures would aid in identifying deficiencies in the future. As the Coast Guard proceeds with its program, another way to improve the submission of paperwork involves educating nonfederal officials about the clearance process.

Interagency Operational Centers Coordinate Harbor Patrols



Source: GAO.

Contents

Letter		1
	Results in Brief	3
	Background	6
	Area Maritime Security Committees Have Improved Information Sharing	11
	Interagency Operational Centers Have Also Improved Information Sharing	16
	Lack of Security Clearances Is a Key Barrier to More Effective Information Sharing	23
	Conclusions	31
	Recommendations for Executive Action	31
	Agency Comments and Our Evaluation	32
Appendix I	Objectives, Scope, and Methodology	34
Appendix II	Stakeholder Groups Recommended for Membership on Area Maritime Security Committees	37
Appendix III	Port-Level Information Sharing Is Supported by, and Supports, National-Level Intelligence Infrastructure	38
Appendix IV	Comments from the Department of Homeland Security	45
Appendix V	GAO Contacts and Staff Acknowledgments	47
	GAO Contacts	47
	Staff Acknowledgments	47
Related GAO Products		48

Tables

Table 1: Representatives That an Area Maritime Security Committee Could Include	37
Table 2: Department and Agency Intelligence Organizations at the National, Regional, and Field Level That Are Potentially Involved in Maritime Information Sharing	38

Figures

Figure 1: Ports Facilitate Cargo Container Traffic, an Important Segment of Maritime Commerce	7
Figure 2: Area Maritime Security Committees Protect a Wide Range of Port Facilities and Adjacent Infrastructure	13
Figure 3: Coast Guard Patrol Enforces Security Zone at a Port	18
Figure 4: Flow of Information from National and Regional Coast Guard Sources to Area Maritime Security Committees and Interagency Operational Centers at the Port Level	42
Figure 5: Flow of Information between National Intelligence and Law Enforcement Agencies and between the National and the Port Level	44

Abbreviations

DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
MTSA	Maritime Transportation Security Act of 2002
OMB	Office of Management and Budget

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

April 15, 2005

The Honorable Henry A. Waxman
Ranking Minority Member
Committee on Government Reform
House of Representatives

The Honorable C. A. Dutch Ruppersberger
The Honorable George Miller
House of Representatives

Securing the nation's ports against a potential terrorist attack has become one of the nation's security priorities since the terrorist attacks of September 11, 2001. Factors that make ports vulnerable to a terrorist attack include their location near major urban centers, such as New York and Los Angeles; their inclusion of critical infrastructure such as oil refineries and terminals; and their economic importance for the nation's economy and trade. Although no port-related terrorist attacks have occurred in the United States, internationally terrorists have demonstrated their ability to access and destroy infrastructure, assets, and lives in and around seaports. According to the Coast Guard, a major port closure for 1 month could cost tens of billions of dollars, disrupting trade and the U.S. economy as a whole.¹

Given that ports are sprawling enterprises that often cross jurisdictional boundaries, the need to share information among federal, state, and local agencies is central to effective prevention and response. The Homeland Security Act of 2002, which provided the basis for federal efforts against terrorism in the aftermath of the September 11 attacks, underscores the importance of sharing timely, effective, and useful information to enhance the shared partnership among federal, state, and local entities in the fight against terrorism.² The act recognizes that sharing information with state and local officials can improve the capability of nonfederal officials to deter, prevent, or disrupt a possible terrorist attack.

¹See U.S. Department of Homeland Security, *U.S. Coast Guard Fiscal Year 2004 Report* (Washington D.C.: February 2004).

²P.L. 107-296, § 891-892 (Nov. 25, 2002).

Since the terrorist attacks, the federal government has taken a number of approaches designed to enhance information sharing.³ One of these approaches, called for under the Maritime Transportation Security Act of 2002 (MTSA), was to provide the Coast Guard with authority for creating area maritime security committees at the port level.⁴ These committees—which were to include representatives from the federal, state, local, and private sectors—were intended as a way to identify and deal with vulnerabilities in and around ports, as well as to provide a forum for sharing information on issues related to port security. Much of the federally generated information about port security—such as assessments of specific port vulnerabilities or information about potential threats being monitored—is classified national security information and cannot be released, even to law enforcement personnel, if they have not undergone the necessary federal background checks and received a security clearance. Lacking access to such information, nonfederal officials may be at a disadvantage in their efforts to respond to or combat a terrorist threat.

As another approach to improving information sharing and port security operations, various federal agencies, including the Department of Homeland Security (through the U.S. Coast Guard), the Department of the Navy, and the Department of Justice (DOJ), have developed interagency operational centers at certain port locations.⁵ These centers are command posts that tie together the intelligence and operational efforts of various federal and nonfederal participants. They currently exist in three locations: Charleston, South Carolina; Norfolk, Virginia; and San Diego, California. Congress has expressed interest in knowing more about the applicability of such centers in other locations, and it required the Coast Guard to submit a report by February 2005 that describes, among other things, the number of ports that could benefit from such centers and the associated cost of implementing them.

³Homeland security information sharing is the two-way exchange of information, including intelligence, critical infrastructure, and law enforcement information, among federal, state, and local governments and the private sector to establish timely, effective, and useful communications to detect, prevent, and mitigate potential terrorist attacks.

⁴The Maritime Transportation Security Act of 2002, P.L.107-295, contains many of the homeland security requirements related specifically to port security. The area maritime security committees are authorized by section 102 of MTSA, as codified at 46 U.S.C. § 70112(a)(2) and implemented at 33 C.F.R. Part 103.

⁵We use the term *interagency operational centers* to refer to centers where multiple federal (and in some cases, state and local) agencies are involved in monitoring maritime security and planning related operations.

The experience gleaned to date from both of these approaches to improving information sharing represents an opportunity that could help guide future efforts to improve port security. Therefore, we examined the efforts of the Coast Guard and other federal agencies in improving information sharing between and among federal, state, local, and industry stakeholders. This report addresses the following questions:

- What impact have area maritime security committees had on information sharing?
- What impact have interagency operational centers had on information sharing?
- What barriers, if any, have hindered improvements in information sharing among port security stakeholders?

To answer these questions, we focused much of our work at the port level. To review the activities of area maritime security committees, we selected four ports for detailed review. These four ports—Baltimore, Maryland; Charleston, South Carolina; Houston, Texas; and Seattle, Washington—were selected to reflect various coastal regions and a wide range of volume and types of operations. To review the activities of the interagency operational centers, we visited all three centers currently in operation, discussing ways in which the centers operate with both federal and nonfederal participants as well as observing operations at the centers. During our visits, we talked with Coast Guard officials involved in sharing information and we also discussed information sharing issues with numerous nonfederal stakeholders, including private sector officials and officials from port authorities or local law enforcement. We examined in more detail the Coast Guard's procedures for processing security clearances for members of area maritime security committees. We also reviewed legislation and congressional committee reports related to information sharing, reviewed numerous other documents and reports on the issue, and spoke with officials at the Coast Guard and the Federal Bureau of Investigation (FBI) about their approaches to sharing information with nonfederal entities. See appendix I for further explanation of our scope and methodology. Our work, which was conducted between May 2004 and March 2005, was done in accordance with generally accepted government auditing standards.

Results in Brief

Area maritime security committees have provided a structure to improve the timeliness, completeness, and usefulness of information sharing

between federal and nonfederal stakeholders. At the four port locations we visited, stakeholders said the newly formed committees were an improvement over previous information sharing efforts because the committees established a formal structure for communicating information and established new procedures for sharing information. Stakeholders stated that among other things, the committees have been used as a forum for sharing assessments of vulnerabilities, providing information on illegal or suspicious activities and providing input on portwide security plans—called area maritime security plans—that describe the joint strategies of the Coast Guard and its partner agencies for protecting key infrastructure against terrorist activities. Nonfederal stakeholders, including state officials, local port authority operators, and representatives of private companies, said the information sharing had increased their awareness of security issues around the port and allowed them to identify and address security issues at their facilities. Likewise, Coast Guard officials said the information they received from nonfederal participants had helped in mitigating and reducing risks. While committees at each of the four locations had the same guidance, they varied in such ways as the size of the membership and the types of stakeholders represented. For example, to prevent a duplication of efforts, some of the committees rely on existing information sharing networks, such as trade and industry associations, and have Coast Guard officials participate directly with these groups, while other ports we visited carried out more of the work in the committee forum. We were not able to determine if certain of these structures or approaches work better than others, largely because the committees are just over a year old. More time will be needed before such assessments can be made.

The three interagency operational centers established to date allow for even greater information sharing because the centers operate 24 hours a day and receive real-time operational information from radars, sensors, and cameras, as well as classified data on personnel, vessels, and cargo, according to center participants. In contrast, the area maritime security committees, while they have a broader membership, primarily provide information through meetings, documents, and other means that are often used for long-term planning purposes rather than day-to-day operations. The three existing interagency centers fulfill varying missions and operations, and thus share different types of information. For example, the center in Charleston, South Carolina, focuses on port security alone and is led by DOJ. In contrast, the center in San Diego supports the Coast Guard's missions beyond port security, including drug interdiction, alien migrant interdiction, and search and rescue activities, and is led by the Coast Guard. The Coast Guard is planning to develop its own operational

centers—called sector command centers—at up to 40 additional port locations to monitor maritime information and to support Coast Guard operations. The relationship between the planned expansion of centers by the Coast Guard and the existing interagency operational centers—in particular, how many other agencies will participate in the Coast Guard’s centers—remains to be determined.

While information sharing has generally improved, a major barrier mentioned most frequently by stakeholders as hindering information sharing has been the lack of federal security clearances among port security stakeholders. The lack of security clearances may limit the ability of state, local, and industry officials, such as those involved in area maritime security committees or interagency operational centers, to deter, prevent, and respond to a potential terrorist attack. By February 2005—or over 4 months after the Coast Guard had developed a list of over 350 nonfederal area maritime security committee participants with a need for a security clearance—28 had submitted the necessary paperwork for the background check. There were two main reasons why the Coast Guard had not processed security clearances more expeditiously. First, local Coast Guard officials said they did not clearly understand their responsibility for communicating with state and local officials about the process for obtaining a security clearance. After receiving a draft of our report, the Coast Guard issued guidelines clarifying the role that local Coast Guard officials play in the program. Second, the Coast Guard had not developed formal procedures for using its database on security clearance applicants to troubleshoot potential problems and take appropriate management action. As the Coast Guard proceeds with its program, nonfederal officials could benefit from more information on the process for obtaining a security clearance. The FBI, which spearheaded a similar effort (but not specific to ports) to expedite security clearances for nonfederal officials, found that nonfederal officials were slow in submitting application forms in part because of the lack of awareness about the security clearance process, and the agency made specific efforts to educate local officials about the application process. Similar educational efforts by the Coast Guard might help clear up any such uncertainties about the application process. Other barriers to greater information sharing identified by committee participants included the size and complexity of ports—factors that are intrinsic to port operations—but none of these barriers were mentioned as frequently and considered as important as the lack of security clearances.

In this report, we recommending that the Secretary of Homeland Security direct the Commandant of the Coast Guard to develop formal procedures

so that local Coast Guard and headquarters officials use the Coast Guard's database as a management tool to monitor who has submitted applications for a security clearance and to take appropriate action when application trends point to possible problems. For example, updating the database on a routine basis could identify port areas where progress is slow and indicate that follow-up with local field office officials may be needed. Finally, we are also recommending that the Coast Guard raise the awareness of state, local, and industry officials about the process of applying for security clearances. This effort could involve using brochures and other information that the FBI has used in its program for educating state and local officials about the security clearance process.

In commenting on a draft of this report, the Department of Homeland Security, including the Coast Guard, generally agreed with our findings and recommendations. The Department of Homeland Security's written comments are in appendix IV.

Background

Ports Are Important and Vulnerable

Ports play an important role in the nation's economy and security. Ports are used to import and export cargo worth hundreds of billions of dollars, generating jobs, both directly and indirectly, for Americans and our trading partners. Ports, which include inland waterways, are used to move bulk agricultural, mineral, petroleum, and paper products. In addition, ports are also used to move cargo containers (as shown in fig. 1)—one of the most important segments of global commerce, accounting for 90 percent of the world's maritime cargo. In 2002, approximately 7 million containers arrived in U.S. seaports, carrying more than 95 percent of the nation's non-North American trade by weight and 75 percent by value. Ports also contribute to the economy through recreational activities such as boating, fishing, and cruises. As an indication of the economic importance of ports, a 2002 simulation of a terrorist attack at a port led to the temporary closure of every seaport in the United States and resulted in an estimated loss of \$58 billion in revenue to the U.S. economy, including spoilage, loss of sales, manufacturing slowdowns, and halts in production.⁶ Ports are also important to national security because they host naval bases

⁶The consulting firm Booz Allen Hamilton and the Conference Board sponsored the simulation in 2002. In the simulation, representatives from government and industry participated in a scenario involving the discovery and subsequent detonation of radioactive bombs hidden in cargo containers.

and vessels, facilitate the movement of military equipment, and supply troops deployed overseas.

Figure 1: Ports Facilitate Cargo Container Traffic, an Important Segment of Maritime Commerce



Source: GAO.

Since the terrorist attacks of September 11, the nation's 361 seaports have been increasingly viewed as potential targets for future terrorist attacks. Ports are vulnerable because they are sprawling, interwoven with complex transportation networks, close to crowded metropolitan areas, and easily accessible. Ports and their maritime approaches facilitate a unique freedom of movement and flow of goods while allowing people, cargo, and vessels to transit with relative anonymity. Because of their accessibility, ports are vulnerable to a wide variety of types of attacks. Cargo containers—mentioned above as important to maritime commerce—are a potential conduit for terrorists to smuggle weapons of mass destruction or other dangerous materials into the country. Finally, ports contain a number of specific facilities that could be targeted by terrorists, including military vessels and bases, cruise ships, passenger ferries, terminals, dams and locks, factories, office buildings, power plants, refineries, sports complexes, and other critical infrastructure.

Multiple Jurisdictions Are Involved in Securing the Nation's Ports

The responsibility for protecting ports from a terrorist attack is a shared responsibility that crosses jurisdictional boundaries, with federal, state, and local organizations involved. For example, at the federal level, the Department of Homeland Security (DHS) has overall homeland security responsibility, and the Coast Guard, an agency of the department, has lead responsibility for maritime security. Other federal departments that may be involved include the Department of Defense (DOD) and DOJ. The Coast Guard and other federal agencies share their security responsibilities with several local stakeholder groups. Some port authorities, operated privately or by the state or local government, have responsibility for protecting certain facilities in and around ports. Port authorities provide protection through designated port police forces, private security companies, and coordination with local law enforcement agencies. Private sector stakeholders play a major role in identifying and addressing the vulnerabilities in and around their facilities, which may include oil refineries, cargo facilities, and other property adjacent to navigable waterways.

Information Sharing Is Important to Port Security Activities

Information sharing among federal, state, and local officials is central to port security activities. The Homeland Security Act of 2002 and several congressionally chartered commissions call attention to the importance of sharing information among officials from multiple jurisdictions as a way to prevent or respond to a terrorist attack.⁷ The act recognizes that the federal government relies on state and local personnel to help protect against terrorist attacks, and these officials need homeland security information to prevent and prepare for such attacks.⁸ One of the congressionally chartered commissioned reports—the 9/11 Commission Report—placed emphasis on the importance of sharing information among federal and nonfederal entities as a means of deterring a terrorist attack in the future. In January 2005, we designated information sharing for homeland security as a high-risk area because the federal government still faces formidable challenges in gathering, identifying, analyzing, and

⁷These congressionally chartered commissions include the 9/11 Commission (the National Commission on Terrorist Attacks upon the United States), the Gilmore Commission (the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction), the Bremer Commission (the National Commission on Terrorism), and the Hart-Rudman Commission (the U.S. Commission on National Security/21st Century).

⁸P.L. 107-296, § 891 (Nov. 25, 2002).

disseminating key information within and among federal and nonfederal entities.⁹

Information sharing between federal officials and nonfederal officials can involve information collected by federal intelligence agencies. In order to gain access to classified information, state and local law enforcement officials generally need to apply for and receive approval to have a federal security clearance. Presidential Executive Order 12968, *Access to Classified Information*, dated August 1995, established federal criteria for granting access to classified information. As implemented by the Coast Guard, the primary criterion for granting access to classified information is an individual's "need to know," which is defined as the determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.¹⁰ To obtain a security clearance, an applicant must complete a detailed questionnaire that asks for information on all previous employment, residences, and foreign travel and contacts that reach back 7 years. After submitting the questionnaire, the applicant then undergoes a variety of screenings and checks by the Coast Guard Security Center. The Office of Personnel Management conducts background investigations on the applicant.

Area Maritime Security Committees Are Established to Facilitate Information Sharing between Port Security Stakeholders

The Maritime Transportation Security Act, passed in the aftermath of the September 11 attacks and with the recognition that ports contain many potential security targets, provided for area maritime security committees to be established by the Coast Guard at ports across the country.¹¹ A primary goal of these committees is to assist the local Captain of the Port—the senior Coast Guard officer who leads the committee—to develop a security plan—called an area maritime security plan—to address the vulnerabilities and risks in that port zone.¹² In developing these

⁹GAO, *High-Risk Series: An Update*, [GAO-05-207](#) (Washington D.C.: January 2005).

¹⁰Executive Order 12968, *Access to Classified Information*, Section 1.1(h).

¹¹See 46 U.S.C. § 70112(a)(2). Prior to MTSA, some port locations had harbor safety committees that had representatives from federal, state, and local organizations. In addition, port security committees had been organized and still exist at ports where substantial out-load and in-load of military equipment occurs.

¹²See 33 C.F.R. § 103.500.

plans, the committees serve as forums to communicate with stakeholders from federal agencies, state and local governments, law enforcement, and private industries in an effort to gain a comprehensive perspective of security issues at a port location. The committees also serve as a link for communicating threats and disseminating security information to port stakeholders. In all, the Coast Guard ultimately organized 43 area maritime security committees, covering the nation's 361 ports.¹³ Besides the Coast Guard, federal agencies such as the Customs and Border Protection, FBI, or Maritime Administration may be part of the committee. State, local, and industry members could include officials from port authorities, oil refineries, and local police or fire departments. Appendix II lists the various stakeholder groups that may be eligible.

To supplement the statutory and regulatory framework of the committees, the Coast Guard developed specific guidelines on communication and collaboration among committee members.¹⁴ This guidance emphasizes the importance of information in successfully implementing security measures and recognizes that the committee structure allows stakeholders to identify other federal, state, and local agencies that are simultaneously developing security standards for other critical infrastructure, such as bridges and airports. The guidance tasks the committee with developing information sharing procedures for various situations, including relaying instances of suspicious activity to appropriate authorities and communicating to port stakeholders threat information, among other things.

Interagency Operational Centers Involve Multiple Participants and Offer Another Means of Improving Information Sharing

Another approach at improving information sharing and port security operations involves interagency operational centers—command centers that bring together the intelligence and operational efforts of various federal and nonfederal participants. These centers provide intelligence information and real-time operational data from sensors, radars, and cameras at one location to federal and nonfederal participants 24 hours a day. The three current centers are in Charleston, South Carolina; Norfolk, Virginia; and San Diego, California. Two of the centers (Norfolk and San Diego) are located in ports that have a substantial number of vessels

¹³Because some ports are located close to one another, some committees cover several ports. For example, the Puget Sound area maritime security committee includes the ports of Seattle, Tacoma, Bremerton, Port Angeles, and Everett.

¹⁴Navigation and Vessel Inspection Circular 9-02, Change 1, Sept. 2002.

and facilities operated by the Department of the Navy. The third center (Charleston) is located at a port that moves military equipment in and out of the port, and it is a major container cargo port.

The development of interagency operational centers represents an effort to improve awareness of incoming vessels, port facilities, and port operations. In general, these centers are jointly operated by federal and nonfederal law enforcement officials. The centers can have command and control capabilities that can be used to communicate information to vessels, aircraft, and other vehicles and stations involved in port security operations.

Port-Level Information Sharing Is Supported by, and Supports, National-Level Intelligence Infrastructure

While area maritime security committees and interagency operational centers are port-level organizations, they are supported by, and provide support to, a national-level intelligence infrastructure. National-level departments and agencies in the intelligence and law enforcement communities may offer information that ultimately could be useful to members of area maritime security committees or interagency operational centers at the port level. These intelligence and law enforcement agencies conduct maritime threat identification and dissemination efforts in support of tactical and operational maritime and port security efforts, but most have missions broader than maritime activities as well. In addition, some agencies also have regional or field offices involved in information gathering and sharing. See appendix III for a description of the departments and agencies or components involved in maritime information sharing at the national and port levels.

Area Maritime Security Committees Have Improved Information Sharing

Area maritime security committees have improved information sharing among port security stakeholders, and made improvements in the timeliness, completeness, and usefulness of information. The types of information shared include assessments of vulnerabilities at specific port locations, information about potential threats or suspicious activities, and strategies the Coast Guard intends to use in protecting key infrastructure. These efforts at sharing information generally did not exist prior to the creation of area maritime security committees. At the ports we visited, the collaboration and sharing of information between committee members reflected the different types of stakeholders and variations in the information needs of each port location. While improvements were noted, it is too early to determine if any one port has developed a better structure for information sharing than another, because the committees have only been operating for just over a year.

Ports Reviewed Showed Improvements in Timeliness, Completeness, and Usefulness of Shared Information

Area maritime security committees have provided a structure to improve the timeliness, completeness, and usefulness of information sharing. For example, a primary function served by the committees was to develop security plans for port areas—called area maritime security plans. The goal of these plans was to identify vulnerabilities to a terrorist attack in and around a port location and to develop strategies for protecting a wide range of facilities and infrastructure (as shown in fig. 2). In doing so, the committees established new procedures for sharing information by holding meetings on a regular basis, issuing electronic bulletins on suspicious activities around port facilities, and sharing key documents, including vulnerability assessments and the portwide security plan itself, according to committee participants. These activities did not exist prior to the creation of the committees, and they have contributed to the improvements in information sharing. The area maritime security plan provides a framework for communication and coordination among port stakeholders and law enforcement officials, and identifies strategies for reducing vulnerabilities to security threats in and near ports. It is designed to capture the information necessary to coordinate and communicate security procedures at each maritime security level, complement and encompass facility and vessel security plans, and ultimately be integrated into the National Maritime Security Plan. Coast Guard officials and nonfederal stakeholders we contacted agreed that efforts such as these have improved information sharing.

Figure 2: Area Maritime Security Committees Protect a Wide Range of Port Facilities and Adjacent Infrastructure



Source: GAO.

Committee participants we spoke with noted that an essential component that has improved the timeliness of information sharing has been the development of both formal and informal stakeholder networks resulting from the formation of area maritime security committees. As part of the process for developing the plan, the committee identifies critical stakeholders and assembles their contact information, allowing for timely dissemination of relevant information. For example, in the event the Coast Guard learns of a potential and credible threat, the committee would designate who should be contacted, the order in which members should be contacted, and what information the committee provides or receives. Participants in the committees told us that the interactions of committee members have also led to the formation of informal stakeholder networks as committee members encounter other stakeholders with similar concerns and perspectives. The committee also provides a forum for real-time sharing of information between stakeholders through meetings or electronic communications. For example, our discussions with federal and nonfederal officials at the ports of Charleston and Houston indicated that

committee members representing private industries were granted access to daily information bulletins that they had not received prior to the formation of area maritime security committees, and these information bulletins have allowed them to stay informed of important Coast Guard decisions. In Houston, the Captain of the Port has used such bulletins to notify and inform local stakeholders of unannounced drills, changes in security levels, and Coast Guard guidance for vessel inspections and voluntary screening. In Charleston, bulletins have been used to share information on closure of waterways, release of new regulations, and methods for preventing a possible terrorist attack.

At the ports we visited, committee members noted that their participation has allowed them to disseminate more complete information and receive more useful information in return. Committee members representing the private sector at two of the ports we visited noted an increased willingness to disclose vulnerabilities to federal stakeholders with confidence that the information would be protected. Coast Guard officials noted that access to more complete information regarding vulnerabilities and threats at individual facilities has aided them in mitigating risks. Additionally, having a complete view of vulnerabilities at the port as a whole has been useful in identifying gaps and common security needs. For example, while private sector stakeholders are sharing their written assessments of their vulnerabilities with the Coast Guard, the Coast Guard is, in turn, sharing its strategies for the overall protection of ports against potential terrorist activities. State and local port authority operators and private sector stakeholders commented that the committees have increased their awareness of security issues around the port and that information received from the Coast Guard has been useful in identifying and addressing security concerns at their facilities. Efforts at sharing information prior to the creation of area maritime security committees had not produced such effects.

Committees Have Flexibility in Their Structure and in the Way in Which They Share Information

While the committees are required to follow the same guidance regarding their structure, purpose, and processes, each of the committees is allowed the flexibility to assemble and operate in a way that reflects the needs of its port area. Each port is unique in many ways, including the geographic area covered and the type of operations that take place there. These port-specific differences influence the number of members that participate, the types of state and local organizations that members represent, and the way in which information is shared.

One aspect of this flexibility is the way in which information is channeled to specific stakeholders. The representation of various stakeholders on a committee can cause differences in the type of information that is shared. While committee members from federal agencies may have access to classified information because they have obtained a security clearance, other members may receive a sanitized version of the information or be restricted from participating in certain committee meetings. To mitigate this situation, some committees have formed subcommittees that deal with classified materials such as intelligence reports or details of military deployments.¹⁵ The role stakeholders play in protecting strategic assets or the type of cargo they handle may also affect what types of information they receive as well as what types of information they can share with the committee at large. For example, at one port we visited, the details regarding a shipment of a sensitive material were restricted to committee members that had a direct involvement in the operation.

The committees also show marked differences in how their meetings occur, and these differences in turn affect the specific ways in which information is shared. For example, at Baltimore, officials told us that committee meetings are open to the general port community and can draw over 80 participants in addition to the 48 committee members. Coast Guard officials told us that such a large attendance made it difficult to conduct committee business. To include all interested stakeholders in the information network while maintaining a working structure for the committee, the Captain of the Port designated 17 members to an executive committee, while the remaining 31 members served on a general committee. This structure allowed the committee to incorporate a large amount of stakeholder input and to share information with all interested parties while keeping the decision making duties of the committee at a manageable level. In contrast to Baltimore's 48 members, the Puget Sound area maritime security committee consists of 25 members who each share in decision making. The smaller committee allows for greater familiarity amongst members as well as immediate decision making at meetings because stakeholders with decision making authority are all present.

At least two of the other committees we reviewed leveraged existing information sharing networks, such as trade and industry associations, by having Coast Guard officials participate in these groups. For example, at

¹⁵The area maritime security committee for the port of Charleston has a separate intelligence subcommittee made up of members that have security clearances.

Charleston, Coast Guard officials noted that many of the stakeholders included on the area maritime security committee were already members of a local maritime association that had been operating since 1926. Officials from the Coast Guard and other federal agencies are members of the association and use the group's meetings as one way of sharing information with stakeholders. Coast Guard officials noted that while this approach may reduce the role and level of participation in the committee, it avoids duplication of efforts and allows the committee to be part of a broader information sharing network. At the port of Houston, the strong presence of the petrochemical industry also made sharing information easier since an association of petrochemical companies was already in place, according to local petrochemical and Coast Guard officials.

Regardless of the structures and communication networks a committee adopted, stakeholders at all four locations we reviewed agreed that the committees fostered improved information sharing. We were not able, however, to determine if any of these structures worked better than others for two reasons. First, the different structures reflected the specific needs of each port location. Second, the committees are still in their early stages of operation and more time will be needed before any comparative assessments can be made.

Interagency Operational Centers Have Also Improved Information Sharing

Interagency operational centers—command centers where officials from multiple agencies can receive data 24 hours a day on maritime activities—have further improved information sharing at three locations. According to participants at each of these centers, the improvements come mainly from the 24-hour coverage and greater amount of real-time, operational data, which the centers can use in their role as command posts for coordinating multi-agency efforts. The Coast Guard is developing plans to develop its own centers, called sector command centers, as part of an effort to reorganize and improve its awareness of the maritime domain. Some of these sector command centers may be interagency on either a regular or an ad hoc basis. However, the potential relationship between interagency operational centers and the Coast Guard's new sector command centers remains to be determined, pending a Coast Guard report to Congress.

Centers Process and Share Information on Operations

Information sharing at the three existing interagency operational centers (Charleston, Norfolk, and San Diego), represents a step toward further improving information sharing, according to participants at all three centers. They said area maritime security committees have improved information sharing primarily through a planning process that identifies

vulnerabilities and mitigation strategies, as well as through development of two-way communication mechanisms to share threat information on an as-needed basis. In contrast, interagency operational centers can provide continuous information about maritime activities and involve various agencies directly in operational decisions using this information. Radar, sensors, and cameras offer representations of vessels and facilities. Other data are available from intelligence sources, including data on vessels, cargo, and crew. For example:

- In Charleston, four federal agencies (DOJ, Coast Guard, U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement) coordinate in a unified command structure, and each of these agencies feeds information into the center. Eight state or local agencies (such as the county sheriff and the state's law enforcement division) have participants at the center full-time, and eight others participate on an as-needed or part-time basis. Federal and nonfederal officials told us that information sharing has improved, since participants from multiple agencies are colocated with each other and work together to identify potential threats by sharing information.
- In San Diego, the center is located in a Coast Guard facility that receives information from radars and sensors operated by the Navy and cameras operated by the local harbor patrol. Local harbor patrol officials are colocated with Coast Guard and Navy personnel. Harbor patrol and Coast Guard staff said the center has leveraged their resources through the use of shared information.
- In Norfolk, the center is staffed with Coast Guard and Navy personnel and receives information from cameras and radars. A Coast Guard Field Intelligence Support Team is colocated at the center and shares information related to the large concentration of naval and commercial vessels in and around the port area with Navy and Coast Guard personnel. According to Coast Guard officials, having a central location where two agencies can receive data from multiple sources on a 24-hour-a-day basis has helped improve information sharing.

Greater information sharing among participants at these centers has also enhanced operational collaboration, according to participants. Unlike the area maritime security committees, these centers are operational in nature—that is, they have a unified or joint command structure designed to receive information and act on it. In the three centers, representatives from the various agencies work side by side, each having access to databases and other sources of information from their respective agencies. The various information sources can be reviewed together, and the

resulting information can be more readily fused together. Officials said such centers help leverage the resources and authorities of the respective agencies. For example, federal and nonfederal participants collaborate in vessel boarding, cargo examination, and other port security responsibilities, such as enforcing security zones (as shown in fig. 3). If the Coast Guard determines that a certain vessel should be inspected on maritime safety grounds and intends to board it, other federal and nonfederal agencies might join in the boarding to assess the vessel or its cargo, crew, or passengers for violations relating to their areas of jurisdiction or responsibility.

Figure 3: Coast Guard Patrol Enforces Security Zone at a Port



Source: GAO.

Variations across Centers Affect Information Sharing

The types of information and the way information is shared varies at the three centers, depending on their purpose and mission, leadership and organization, membership, technology, and resources, according to officials at the centers. The Charleston center has a port security purpose, so its missions are all security related. It is led by DOJ, and its membership

includes 4 federal agencies and 16 state and local agencies. The San Diego center has a more general purpose, so it has multiple missions to include, not just port security, but search and rescue, environmental response, drug interdiction, and other law enforcement activities. It is led by the Coast Guard, and its membership includes two federal agencies and one local agency. The Norfolk center has a port security purpose, but its mission focuses primarily on force protection for the Navy. It is led by the Coast Guard, and its membership includes two federal agencies and no state or local agencies. As a result, the Charleston center shares information that focuses on law enforcement and intelligence related to port security among a very broad group of federal, state, and local agency officials. The San Diego center shares information on a broader scope of activities (beyond security) among a smaller group of federal and local agency officials. The Norfolk center shares the most focused information (security information related to force protection) among two federal agencies. While the Norfolk center officials said they were planning to broaden the scope of their purpose, mission, and membership, they had not done so at the time of our visit.

The centers also share different information because of their technologies and resources. The San Diego and Norfolk centers have an array of standard and new Coast Guard technology systems and access to Coast Guard and various national databases, while the Charleston center has these as well as additional systems and databases. For example, the Charleston center has access to and shares information on Customs and Border Protection's databases on incoming cargo containers from the National Targeting Center. In addition, Charleston has a pilot project with the Department of Energy to test radiation detection technology, which provides additional information to share. The Charleston center is funded by a special appropriation that allows it to use federal funds to pay for state and local agency salaries. This arrangement boosts the participation of state and local agencies, and thus information sharing beyond the federal government, according to port stakeholders in Charleston. While the San Diego center also has 24-hour participation by the local harbor patrol, that agency pays its own salaries.

Other Ad Hoc Arrangements for Interagency Information Sharing

In addition to the three interagency operational centers we visited, our work has identified other interagency arrangements that facilitate information sharing and interagency operations in the maritime environment. One example is a predesignated single-mission task force, which becomes operational when needed. DHS established the Homeland Security Task Force, South-East—a working group consisting of federal

and nonfederal agencies with appropriate geographic and jurisdictional responsibilities that have the mission to respond to any mass migration of immigrants affecting southeast Florida. Task force members (both agencies and individuals) are predesignated, and they have a contingency plan (called Vigilant Sentry) that describes each agency's specific coordination and mission responsibilities. The task force meets regularly to monitor potential migration events, update the contingency plan, and otherwise coordinate its activities. When a mass migration event occurs, the task force is activated and becomes a full-time interagency effort to share information and coordinate operations to implement the contingency plan. This task force was activated in February 2004 to implement Operation Able Sentry to interdict a mass migration from Haiti.

Another example of an interagency arrangement for information sharing can occur in single-agency operational centers that become interagency to respond to specific events. For example, the Coast Guard has its own command centers for both its District Seven and Sector Miami. While these centers normally focus on a variety of Coast Guard missions and are not normally interagency in structure, they have established protocols with other federal agencies, such as Customs and Border Protection and Immigration and Customs Enforcement, to activate a unified or incident command structure should it be needed. For example, the interagency Operation Able Sentry (discussed above) was directed from the Coast Guard's District Seven command center. Similarly, to respond to a hijacking of a ship, an interagency operation was directed from the Coast Guard's Sector Miami command center. While an interagency operation might be directed from these Coast Guard command centers, it might be led by another agency with greater interests or resources to respond to an event. For example, this was the case with a recent interagency operation to arrange for the security of dignitaries at an international conference in Miami that was led by Immigration and Customs Enforcement. These Coast Guard centers make it possible to host interagency operations because they have extra space and equipment that allow for surge capabilities and virtual connectivity with each partner agency.

Officials from the Coast Guard, Customs and Border Protection, and Immigration and Customs Enforcement in Miami all said that these ad hoc interagency arrangements were crucial to sharing information and coordinating operations.

Coast Guard Plans to Develop Sector Command Centers at Ports

The Coast Guard is planning to develop its own operational centers—called sector command centers—at additional ports. These command centers are being developed to provide local port activities with a unified command as the Coast Guard reorganizes its marine safety offices and groups into unified sectors. In addition, the Coast Guard sector command centers are designed to improve awareness of the maritime domain through a variety of technologies. The Coast Guard is planning to have command centers feed information to the Coast Guard's two area offices—one on the Pacific Coast and the other on the Atlantic Coast. Over the long term, the Coast Guard plans to have information from sector command centers and area offices channeled to a center at the national level—allowing the Coast Guard to have a nationwide common operating picture of all navigable waters in the country. A Coast Guard official indicated that this nationwide information will be available to other field office commanders at the same time it is given to area and headquarters officials. To develop this nationwide operating picture, the Coast Guard hopes to install equipment that allows it to receive information from sensors, classified information on maritime matters, and data related to ships and crewmembers as part of its expansion plans. Communication from Coast Guard ships and aircraft, as well as federal and nonfederal systems for monitoring vessel traffic and identifying the positions of large ships, would be among the other types of information that could be integrated into a command center.

The Coast Guard plans to develop sector command centers at 10 port locations, with potential expansion to as many as 40 port locations. The Coast Guard is currently conducting site surveys to identify locations where it believes centers should be located. For fiscal year 2006, the Coast Guard is requesting funds that support its plans to improve awareness of the maritime domain by, among other things, continuing to evaluate the potential expansion of sector command centers to other port locations. For example, the Coast Guard's budget request includes \$5.7 million to continue developing a nationwide maritime monitoring system, the common operational picture. The common operational picture is primarily a computer software package that fuses data from different sources, such as radar, sensors on aircraft, and existing information systems. The Coast Guard has also requested funding for training personnel in common operational picture deployment at command centers and to modify facilities to implement the picture in command centers. While the total cost of operating command centers is still unknown, the Coast Guard's Five-Year Capital Investment Plan shows that the capital costs of this effort amount to an estimated \$400 million, with acquisition of the system estimated to start in fiscal year 2007.

Coast Guard Report Pending on Interagency Operational Centers

The relationship between the interagency operational centers and the Coast Guard's sector command centers has not been determined yet. Coast Guard sector command centers can involve multiple agencies, and the Coast Guard has begun using the term "sector command center—joint" for the interagency operational centers in San Diego and Norfolk. Coast Guard officials have told us that their planned sector command centers will be the basis for any interagency operational centers at ports. However, the sector command center we visited, in Sector Miami, was not interagency on a routine basis—the Coast Guard is the single entity operating the center.

During our visits to the interagency operational centers, port stakeholders raised the following issues as important factors to consider in any expansion of interagency operational centers: (1) purpose and mission—the centers could serve a variety of overall purposes, as well as support a wide number of specific missions; (2) leadership and organization—the centers could be led by several departments or agencies and be organized a variety of ways; (3) membership—the centers could vary in membership in terms of federal, state, local, or private sector participants and their level of involvement; (4) technology deployed—the centers could deploy a variety of technologies in terms of networks, computers, communications, sensors, and databases; and (5) resource requirements—the centers could also vary in terms of resource requirements, which agency funds the resources, and how resources are prioritized.

In a related step, Congress directed the Coast Guard to report on the existing interagency operational centers, covering such matters as the composition and operational characteristics of existing centers and the number, location, and cost of such new centers as may be required to implement maritime transportation security plans and maritime intelligence activities.¹⁶ This report, which Congress called for by February 2005, had not been issued by the time we had completed our work and prepared our report for printing. According to DHS, the report has been written and has been approved by DHS and the Office of Management and Budget (OMB), and is now in the final stages of review at the Coast Guard. Until the report on the centers is issued, it is unclear how the Coast Guard

¹⁶See The Coast Guard and Maritime Transportation Act of 2004, P.L. 108-293, § 807 (August 9, 2004). While the statute uses the term "joint operational centers," we are using the term "interagency operational centers" to denote centers where multiple agencies participate. According to Coast Guard officials, the term "joint" refers to command centers where the Coast Guard and Navy are involved in carrying out the responsibilities of the center.

will define the potential relationship between interagency operational centers and its own sector command centers.

Lack of Security Clearances Is a Key Barrier to More Effective Information Sharing

The lack of security clearances was most frequently cited as a barrier to more effective information sharing among port stakeholders, such as those involved in area maritime security committees and interagency operational centers. The Coast Guard has initiated a security clearance program for members of area maritime security committees. However, the results of the Coast Guard's efforts have been mixed. For example, only a small percentage of application forms from state, local, and industry officials had actually been submitted by February 2005—over 4 months after the Coast Guard had developed its list of officials. The primary reason given for this was that Coast Guard field office officials did not clearly understand their role in helping nonfederal officials apply for a security clearance. The Coast Guard's program does not have formal procedures for using data to manage the program, but developing such procedures would allow the Coast Guard to identify and deal with possible problems in the future. Finally, as the Coast Guard moves forward with its state, local, and industry security clearance program, the experience of other federal agencies that manage similar programs suggests that the limited awareness of state, local, and industry officials about the process for obtaining a security clearance could also impede the submission of applications for a security clearance.

Port Security Stakeholders Cite the Lack of Clearances as a Problem

At the ports we visited, the lack of security clearances was cited as a key barrier to information sharing among participants of area maritime security committees and interagency operational centers we contacted. Port stakeholders involved in the four area maritime security committees consistently stated that the lack of federal security clearances for nonfederal members was an impediment to effective information sharing. Here are several examples:

- An official of the Washington State Ferries who participates on the Puget Sound area maritime security committee said that not having a security clearance—and therefore the ability to access classified information—affected his ability to carry out security-related activities.¹⁷ He noted that the local U.S. Attorney reported to a local

¹⁷Washington State Ferries is the largest state-operated ferry system in the country.

newspaper in the summer of 2004 that suspicious activities had been reported on the state ferry system. The Washington State Ferries official indicated that he or his staff was the source for some of the data but that federal officials would not provide him with more details on the activities because he did not have a security clearance. A Coast Guard field intelligence official corroborated this by stating that the Captain of the Port was unable to share classified information from the U.S. Attorney's office that indicated a pattern of incidents involving the ferries. Although Coast Guard officials said they wanted to share this information, ferry officials' lack of a federal security clearance precluded them from doing so. Both Coast Guard and ferry officials indicated that more complete information would aid local security officers in identifying or deterring illegal activities.

- A senior Maryland state official involved in making budget decisions on improving security around facilities in the port of Baltimore indicated that having a security clearance would aid his ability to make decisions on how the state could more effectively spend its resources on homeland security. He said information on what transportation sectors are probable targets would be a valuable input on where the state should prioritize its spending decisions.
- A senior Coast Guard official in Houston told us that granting security clearances to selected members of the area maritime security committee would make it easier for nonfederal officials to make decisions on how to respond to specific threats. A local Coast Guard intelligence official cited an example in which classified information could not be shared with port stakeholders. The official told us that there were delays in sharing the information until the originator of the information supplied a sanitized version.

Similar to the concerns expressed by area maritime security committee members, participants we contacted at the three interagency operational centers cited the lack of security clearances as a barrier to information sharing. At the center in San Diego, the chief of the local harbor patrol noted that the lack of security clearances was an issue for patrol staff who are involved in the center. Subsequent to raising this issue, DHS sponsored security clearances for 18 harbor patrol officials. At the center in Charleston, participants in the interagency operational center cited the lack of security clearances as a potential barrier to information sharing. The Department of Justice addressed this potential barrier by granting security clearances to nonfederal officials involved in the center. Finally, Coast Guard officials indicated that when nonfederal officials begin working at the interagency operational center in Norfolk, granting security

clearances to nonfederal participants will be critical to their success in sharing information.

According to the Coast Guard and state and local officials we contacted, the shared partnership between the federal government and state and local entities may fall short of its potential to fight terrorism because of the lack of security clearances. If state and local officials lack security clearances, the information they possess may be incomplete. According to Coast Guard and nonfederal officials, the inability to share classified information may limit their ability to deter, prevent, and respond to a potential terrorist attack.

While security clearances for nonfederal officials who participate in interagency operational centers are sponsored by DOJ and DHS, the Coast Guard sponsors security clearances for members of area maritime security committees. For the purposes of our review, we examined in more detail the Coast Guard's efforts to address the lack of security clearances among members of area maritime security committees.

Coast Guard Has Taken Steps to Grant Additional Clearances to State, Local, and Industry Officials, but Efforts to Date Have Been Mixed

As part of its effort to improve information sharing at ports, the Coast Guard initiated a program in July 2004 to sponsor security clearances for members of area maritime security committees, but nonfederal officials have been slow in submitting their applications for a security clearance. By October 2004, the Coast Guard had identified 359 nonfederal committee members who had a need to know and should receive a security clearance, but as of February 2005, only 28 officials, or about 8 percent, had submitted the application forms for a security clearance. Twenty-four of these officials have been granted an interim clearance, which allows access to classified material while the final clearance is being processed.

We interviewed local Coast Guard officials at the four ports we visited to gain a better understanding of the role of the Coast Guard in guiding state and local officials through the process. Our work shows that there were two areas that affected the Coast Guard's efforts: (1) local Coast Guard officials did not clearly understand their role in the security clearance program and (2) the Coast Guard did not use available data to track the status of security clearances for state and local officials.

Coast Guard Field Office
Officials Said They Did Not
Clearly Understand Their Role
in the Security Clearance
Program

Coast Guard field office officials said they did not clearly understand their role in helping nonfederal officials apply for a security clearance. In July 2004, Coast Guard headquarters sent guidance to Coast Guard field offices requesting them to proceed with submissions of personnel security investigation packages and to submit the additional names of state and local officials who had a need for a security clearance. However, this guidance evidently was unclear to field office officials. For example, by January 2005—3 months after they submitted names to headquarters—Coast Guard officials at three of the ports we visited were still awaiting further guidance from headquarters on how to proceed.¹⁸ These officials said they thought that headquarters was processing security clearances for nonfederal officials, and they were waiting for notification from headquarters that security clearances had been granted.

Our discussions with a Coast Guard field office official at the fourth port location suggest that additional guidance about the process for the state, local, and industry security clearance program could be beneficial. For example, according to this official, membership on area maritime security committees changes over time, and it would be helpful to have guidance on the process for obtaining additional security clearances or dropping clearances for officials who no longer participate on the committees or who no longer have a need to know classified information. This official noted that the process differed depending on whether a committee participant is considered to be a military or civilian official.

In early February 2005, we expressed our concerns about the security clearance program to Coast Guard officials. On the basis, in part, of our discussions, Coast Guard headquarters took action and drafted guidance informing its field office officials that they were responsible for contacting nonfederal officials and for providing them with application forms for obtaining a security clearance, according to Coast Guard officials. Additionally, to further clarify the role of field office officials, the Coast Guard's draft guidance included information on various procedures for obtaining a security clearance. After receiving a draft of this report, the Coast Guard finalized this guidance and sent it to field office officials in early April 2005. Our review of the guidance shows that it clarifies the role of field office officials in administering the security clearance process at

¹⁸ At the fourth location, the local Coast Guard official initiated contact with nonfederal officials on his own, and he asked for additional information from headquarters. At this location, the field office is working with nonfederal officials to submit their application forms or to verify that they already have a security clearance.

the local level and that it provides more detailed procedures on how to check the status of applications that have been submitted for a security clearance.

In addition to writing draft guidance on the program, the Coast Guard recently demonstrated that the security clearance program has produced some positive results. For example, in late 2004, the Coast Guard determined the need to share the results of a security study on ferries, portions of which were classified, with some members of an area maritime security committee. Working with Coast Guard field office officials, Coast Guard headquarters and the Coast Guard Security Center were able to process and grant about a dozen security clearances to state, local, and industry officials. As a result, the Coast Guard was able to share classified information with state, local, and industry officials that it believed would help them in carrying out their port security responsibilities.

Data Could Be More Effectively Used as a Tool to Manage the Security Clearance Program

A key component of a good management system is to have relevant, reliable, and timely information available to assess performance over time and to correct deficiencies as they occur. The Coast Guard has two databases that contain information on the status of security clearances for state, local, and industry officials. The first database is a commercial off-the-shelf system that contains information on the status of all applications that have been submitted to the Coast Guard Security Center, such as whether a security clearance has been issued or whether personnel security investigations have been conducted. In February 2004, the Coast Guard began testing the database for use by field staff, and while headquarters has still not granted field staff access to the database, it plans to do so in the future. The second database—an internally developed spreadsheet on the 359 area maritime committee participants—summarizes information on the status of the security clearance program, such as whether they have submitted their application forms and whether they have received their clearances.

Although the Coast Guard has databases that could be used to manage the state, local, and industry security clearance program, thus far, it has not developed formal procedures for using the data as a management tool to follow up on possible problems at the national or local level to verify the status of clearances. In regard to the database used by the Security Center, a Coast Guard official told us that the database was not designed to monitor application trends, but instead is used to provide information on individual applicants. The Coast Guard's internally developed spreadsheet on committee participants who have been deemed candidates for a security clearance, however, does offer information on application trends,

and could be used to monitor progress that has been made at the national or local level. For example, updating the database on a routine basis could identify port areas where progress is slow and indicate that follow-up with local field office officials may be needed. In a similar security clearance program, the experience of the FBI shows the utility of data as a tool for managing the program. For example, FBI officials indicated that its databases have served as management tools for tracking state, local, and industry security applications and for monitoring application trends and percentages. The Coast Guard has yet to develop formal procedures for using its data on committee participants as a tool to assess potential problems and to take appropriate action, if necessary. Doing so would likely aid its efforts to manage the state, local, and industry security clearance program at both the local and the national levels.

While the Coast Guard's databases on security clearances shows promise as a tool for monitoring the state, local, and industry security clearance program, the database also has limitations in that it cannot be used to determine how many nonfederal officials have a federal security clearance sponsored by other federal agencies. For example, a Coast Guard official stated that this information is difficult to obtain because the Coast Guard does not have easy access to databases of other agencies. In September 2004, we testified that existing impediments to managing the security clearance process include the lack of a governmentwide database of clearance information, which hinders efforts to provide timely, high-quality clearance determinations.¹⁹ As a way to deal with this problem, a local Coast Guard official sent a survey to port security stakeholders to determine how many stakeholders had security clearances sponsored by other federal agencies.

Raising the Awareness of State, Local, and Industry Officials Might Improve the Processing of Application Forms

Our prior reviews of DOD and FBI efforts to manage a large number of security clearances for service members, government employees, and industry personnel have demonstrated long-standing backlogs and delays. In addition, our FBI work showed that it is important to address training and education to successfully carry out an effective security clearance

¹⁹GAO, *Intelligence Reform: Human Capital Considerations Critical to 9/11 Commission's Proposed Reforms*, [GAO-04-1084T](#) (Washington, D.C.: September 14, 2004).

program.²⁰ Our reviews also showed that the use of internal controls to ensure that security clearances are granted in compliance with existing rules and regulations will become increasingly important.

The experience of the FBI in managing its security clearance program shows that educating nonfederal officials about the security clearance program resulted in improvements in the processing of applications for a security clearance. The FBI grants security clearances to state and local law enforcement officials who may require access to classified national security information to help prevent or respond to terrorist attacks. After September 11, an increasing number of state and local officials began requesting security clearances to obtain terrorism-related information that might affect their jurisdictions. However, when the FBI received a low percentage of application forms for security clearances from nonfederal officials, the agency consulted with state and local officials to collect their views and recommendations regarding information sharing and improving the security clearance process, and the FBI identified unfamiliarity with the requirements for processing security clearance applications as one of the main impediments to timely processing of applications. For example, some state and local officials said that they did not have adequate guidance for filling out and submitting the appropriate application forms. In response, the FBI widely distributed step-by-step guidance to state and local law enforcement officials through informational brochures (available on a FBI Web site) and meetings with state and local officials, among other efforts. Some law enforcement officials we interviewed stated that the FBI's guidance and consultation with law enforcement professional organizations helped improve state and local officials' understanding of the security clearance application process.²¹

Once the Coast Guard begins notifying more state, local, and industry officials about the process for obtaining a security clearance, raising the awareness of nonfederal officials about the program could improve the processing of application forms. An official at the field office that had

²⁰ GAO, *DOD Personnel Clearances: Preliminary Observations Related to Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel*, [GAO-04-202T](#) (Washington, D.C.: May 6, 2004); *Aviation Security: Federal Air Marshal Service Is Addressing Challenges of Its Expanded Mission and Workforce, but Additional Actions Needed*, [GAO-04-242](#) (Washington, D.C.: Nov. 19, 2003); and *Security Clearances: FBI Has Enhanced Its Process for State and Local Law Enforcement Officials*, [GAO-04-596](#) (Washington, D.C.: Apr. 30, 2004).

²¹ [GAO-04-596](#), p.24.

actually contacted state and local officials about the security clearance program indicated that field office officials did not have basic information about the security clearance program. Among other things, he mentioned that informational brochures and Web sites could be given to nonfederal officials as a way to improve their awareness of the security clearance process.

Attending to the potential lack of awareness by nonfederal officials about the security clearance program is important because the number of nonfederal officials who submit application forms for a security clearance may be much larger than the several hundred state, local, and industry officials who participate on area maritime security committees. For example, DHS will sponsor an estimated 5,000 security clearances for state, local, and industry officials and the Coast Guard Security Center will process these clearances, according to Coast Guard officials. Additionally, the Coast Guard plans to grant clearances to about 200 other nonfederal officials who are involved in supporting other Coast Guard operations, such as sector command centers. In addition, as the Coast Guard's security clearance program evolves, participants on area maritime security committees or in sector command centers may change over time, thus highlighting the importance of having ways to raise the awareness of nonfederal officials about the security clearance process.

Other Barriers Intrinsic to Port Operations May Also Impede Information Sharing

Port security stakeholders cited other barriers to effective information sharing intrinsic to ports we visited, but none of these barriers were mentioned as frequently as the lack of security clearances. At the four ports we visited, characteristics intrinsic to the port, such as their size and complexity were stated as barriers to effective information sharing. In Houston, for example, multiple stakeholders, such as port authorities, numerous jurisdictions, and a diverse set of users, were presented as challenges in information sharing efforts. The length of the Houston Ship Channel (50 miles), with numerous public and private entities using the channel, also complicates information sharing efforts. To deal with the size and complexity of this port area, Coast Guard officials said they have worked with associations representing the commercial fishing industry, petrochemical companies, and state and local law enforcement as a means to share information about port security with as many users of the port and the Houston Ship Channel as possible. For example, the local Coast Guard officials said they held informational meetings with recreational boating associations and with area maritime security committee participants to inform boaters and other stakeholders of "safety zones"—areas where recreational use of the waterway is prohibited—in the

Houston Ship Channel. Another barrier mentioned at another port location was the “cultural” barrier between various members of the area maritime security committees. For example, officials at this port location stated that an informal network has created insiders and outsiders drawing particular distinctions between law enforcement and non-law enforcement officials.

Conclusions

Effective information sharing among members of area maritime security committees and participants in interagency operational centers can enhance the partnership between federal and nonfederal officials, and it can improve the leveraging of resources across jurisdictional boundaries for deterring, preventing, or responding to a possible terrorist attack at the nation’s ports. The Coast Guard has recognized the importance of granting security clearances to nonfederal officials as a means to improve information sharing, but progress in moving these officials through the application process has been slow. In the future, the Coast Guard may need to grant additional security clearances to state, local, or industry participants who join area maritime security committees or sector command centers to support counterterrorism programs. In this way, as the Coast Guard’s state, local, and industry security clearance program matures, the importance of effectively managing the security clearance program will become even more important. Increased management attention and guidance about the process would strengthen the program for security clearances, and it would reduce the risk that nonfederal officials may have incomplete information as they carry out their law enforcement activities.

Recommendations for Executive Action

To help ensure that nonfederal officials receive needed security clearances as quickly as possible, both now and in the future, we recommend that the Secretary of Homeland Security direct the Commandant of the Coast Guard to take the following two actions.

- Develop formal procedures so that local and headquarters officials use the Coast Guard’s internal databases of state, local, and industry security clearances for area maritime committee members as a management tool to monitor who has submitted applications for a security clearance and to take appropriate action when application trends point to possible problems. For example, updating the database on a routine basis could identify port areas where progress is slow and indicate that follow-up with local field office officials may be needed.

-
- Raise the awareness of state, local, and industry officials about the process of applying for security clearances. This effort could involve using brochures, Web sites, or other information that the FBI has used in its program for educating state and local officials about the security clearance process.

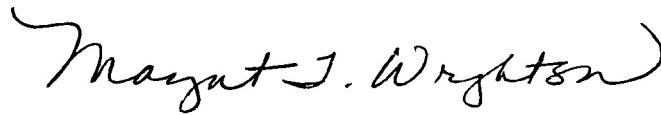
Agency Comments and Our Evaluation

We provided a draft of this report to DHS, DOJ, and DOD for comment. DHS, including the Coast Guard, generally agreed with our findings and recommendations. Specifically, DHS noted that our recommendations should enhance the Coast Guard's efforts to promote information sharing among port security stakeholders. DHS also indicated that changes associated with processing security clearances should overcome identified impediments. DOJ and DOD declined to provide comments.

Our draft report included a recommendation that the Coast Guard clarify the role of field office officials in communicating with state, local, and industry officials about the process for obtaining a security clearance. After receiving our draft report, the Coast Guard issued a memo to field office officials that clarified their role in the security clearance program. The Coast Guard's memo also provided more detailed guidance on the process for sponsoring additional state, local, or industry officials for a security clearance. As a result of the Coast Guard's action, we have dropped this recommendation from our final report. In regard to interagency operational centers, DHS also noted that the Coast Guard report required by Congress on existing interagency operational centers has been approved by DHS and OMB and is now in the final stages of review at the Coast Guard. In addition to commenting on our findings and recommendations, DHS provided technical comments on the report under separate cover and we revised the draft report where appropriate. Written comments from DHS are reprinted in appendix IV.

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its issue date. At that time, we will provide copies of this report to appropriate departments and interested congressional committees. We will also make copies available to others upon request. This report will also be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any question about this report, please contact me at (415) 904-2200 or at wrightsonm@gao.gov or Stephen L. Caldwell, Assistant Director, at (202) 512-9610 or at caldwells@gao.gov. Key contributors to this report are listed in appendix V.

A handwritten signature in black ink that reads "Margaret T. Wrightson". The signature is fluid and cursive, with the first name "Margaret" and last name "Wrightson" clearly legible.

Margaret T. Wrightson
Director, Homeland Security
and Justice Issues

Appendix I: Objectives, Scope, and Methodology

Each of our objectives involved information sharing between federal agencies and nonfederal stakeholders. Specifically,

- What impact have area maritime security committees had on information sharing?
- What impact have interagency operational centers had on information sharing?
- What barriers, if any, have hindered improvements in information sharing among port security stakeholders?

We carried out part of our work at Coast Guard headquarters or in consultation with headquarters officials. We spoke with Coast Guard officials to obtain information on how information is shared within the maritime security community and reviewed pertinent legislation, guidance, rules, and other relevant documents related to the sharing of maritime security information with nonfederal stakeholders. For example, we reviewed pertinent statutes, such as the Maritime Transportation Security Act and the Homeland Security Act. We also reviewed selected maritime security plans, Coast Guard regulations implementing the Maritime Transportation Security Act, and various reports from congressionally chartered commissions related to information sharing.

To address our first objective, we conducted structured interviews with officials from federal agencies and representatives from state and local governments, law enforcement agencies, maritime industry associations, and private sector entities who were stakeholders in port security issues. Many of these officials were members of area maritime security committees. These interviews were largely conducted during site visits to four specific maritime port areas. We selected these ports to provide a diverse sample of security environments and perspectives, basing our selections on such matters as geographic location, varying levels of strategic importance, and unique local characteristics. The four port areas and some of our reasons for choosing them are as follows:

- Baltimore, Maryland: a Mid-Atlantic port that is managed by a state agency and services a variety of cargo, including bulk and container cargo, and cruise passengers;
- Charleston, South Carolina: a South Atlantic port that is state owned and operated, with three separate facilities and military facilities and installations;

- Houston, Texas: a Gulf coast port that is governed by an appointed commission and consists of a 25-mile-long complex of diversified public and private facilities, including the nation's largest petrochemical complex; and
- Seattle/Tacoma, Washington: a Pacific coast port area that is operated by municipal corporations, represents the third largest container cargo port in the country, and services the country's largest state-operated passenger ferry system.

During each of our visits to these four ports, we met with the identified port stakeholders, Coast Guard marine safety offices, and Captains of the Port. In our meetings with Captains of the Port and marine safety offices, we discussed the creation of and composition of the area maritime security committee at their port and the effectiveness of the committee in facilitating information sharing. We also discussed and collected documents related to policies and procedures pertaining to sharing information with nonfederal stakeholders. We collected documentary evidence in the form of information bulletins that are used to disseminate information to stakeholders. When we met with the nonfederal stakeholders at the ports, we discussed specific security concerns at their facilities or in their jurisdictions and how they were being addressed. We also discussed their involvement and experiences with the local area maritime security committee, of which most were members, and how they receive and share information with federal agencies, particularly the Coast Guard. With both groups, we discussed any perceived barriers to information sharing and ideas and plans to resolve these issues. This information was used in conducting a comparative analysis of the port areas and allowed us to distinguish differences between the locations while identifying common issues.

In addressing the second objective, we conducted site visits at the three interagency operational centers located in Charleston, South Carolina; Norfolk, Virginia; and San Diego, California. Related to this, we visited the Homeland Security Task Force South-East and command centers for the Coast Guard district and sector in Miami, Florida because these centers also aim to facilitate information sharing and joint operations related to maritime security. At each location, we conducted structured interviews with officials from the agencies participating in the centers. These interviews allowed us to obtain information regarding the history of the centers and how their missions and structures are changing. Specifically, we discussed how their presence affects information sharing among federal stakeholders as well as with nonfederal stakeholders. We also

discussed challenges facing the centers as they become more formalized. During the visits, documents that describe the centers as well as examples of the products they distribute were collected. Observations made at the facilities allowed us to provide context to the testimonial evidence we collected. We also viewed demonstrations of the emerging technologies as well as differences in the physical attributes of each center. The testimonial evidence, aided by our observations, was synthesized and analyzed, allowing us to perform a comparative analysis, identifying differences and commonalities in information sharing among the centers.

To address the third objective, we followed up with officials at Coast Guard headquarters and obtained guidance and data regarding the current effort to administer security clearances at the secret level to selected nonfederal stakeholders at each port. In subsequent phone interviews with the officials of marine safety offices at the ports we visited, we discussed problems encountered in the communication and implementation of this effort and steps that are being taken to resolve these problems. In addition, we reviewed Coast Guard documents related to information sharing, such as data on the number of nonfederal officials who had received security clearances, guidance from Coast Guard headquarters to field offices, and other pertinent instructions. In regard to this database, we checked the reliability of the database for the four ports we visited and found that the database was generally accurate. We found that 24 of the 27 entries were correct. In addition, we reviewed prior GAO reports that dealt with information sharing issues. Finally, we interviewed 64 federal and nonfederal stakeholders at the four ports we visited and asked them whether there were any barriers to information sharing. The results of our interviews cannot be projected to all participants on the area maritime security committees.

Our review was conducted from May 2004 to March 2005 in accordance with generally accepted government auditing standards.

Appendix II: Stakeholder Groups Recommended for Membership on Area Maritime Security Committees

This appendix provides information on the Coast Guard’s guidance for developing the local membership and organization of the area maritime security committee. The Coast Guard’s guidance directs the Captain of the Port to take into account all aspects of each port area and its adjacent waterways and coastal areas. The committees should be composed of federal, state, and local agencies; law enforcement and security agencies; and port stakeholders. Representatives for each aspect of the port and those charged with its regulation or enforcement should be encouraged to participate. Table 1 provides a list of representatives that an area maritime security committee could include.

Table 1: Representatives That an Area Maritime Security Committee Could Include		
Federal agencies	State and local agencies	Industry-related agencies
U.S. Coast Guard (USCG)	National Guard	Facility owners/operators
Department of Defense (DOD)	Marine police	Terminal owners/operators
Nuclear Regulatory Commission (NRC)	Port authority police and security forces	Trade organizations
U.S. Department of Agriculture (USDA)	Fire departments	Recreational boating organizations (yacht clubs, rowing clubs)
Environmental Protection Agency (EPA)	Civil defense	Railroad companies
Occupational Safety and Health Agency (OSHA)	City government officials	Trucking companies
Federal Bureau of Investigation (FBI)	Transportation agencies	Shipyards
Emergency Preparedness and Response (EPR)	Fish and wildlife marine units	Tow-boat operators
Customs and Border Protection (CBP)	Health agencies	Marine exchanges
Immigration and Customs Enforcement (ICE)	Occupational safety agencies	Industry organizations
Transportation Security Administration (TSA)	Terminal/facility security forces	Organized labor
Army Corps of Engineers (ACOE)	Pilot associations	Commercial fishing industry
U.S. Transportation Command (TRANSCOM)	Other state, local, and city government representatives	Waterborne vendors and service providers (harbor tugs, launch services, line handlers, small ferry operators, water taxis)
Military Sealift Command (MSC)	State department of natural or environmental resources marine units	Other facilities within the port having waterside access, e.g., refineries, chemical plants, power plants
Military Traffic Management Command (MTMC)	Other environmental agencies	
Animal and Plant Health Inspection Service (APHIS)	Regional development agencies/ metropolitan planning organizations	
Maritime Administration (MARAD)		
Research and Special Programs Administration (RSPA)		
Federal Railway Administration (FRA)		
Federal Highway Administration (FHWA)		
Federal Transit Administration (FTA)		
Other government representatives, where appropriate		

Source: Coast Guard.

Area maritime security committees are not limited to the agencies and organizations on this list. As each port has specific needs and issues, the membership of committees can vary greatly from port to port.

Appendix III: Port-Level Information Sharing Is Supported by, and Supports, National-Level Intelligence Infrastructure

This appendix provides information on the departments and agencies/components involved in maritime information sharing, at both the national level and the regional or field level. Table 2 lists departments and agencies/components (including the Coast Guard) that potentially play a role in disseminating maritime threat information to, and receiving information from, area maritime security committees and interagency operational centers.

Table 2: Department and Agency Intelligence Organizations at the National, Regional, and Field Level That Are Potentially Involved in Maritime Information Sharing

Department and agency/component	National-level intelligence organizations	Regional or field-level intelligence organizations
Department of Homeland Security		
U.S. Coast Guard (USCG)	The Coast Guard Intelligence Coordination Center (ICC), working in conjunction with the Navy’s Office of Naval Intelligence (ONI) at the National Maritime Intelligence Center (NMIC), tracks the movement of vessels, cargoes, and crews while providing intelligence analysis and warning information.	Two Coast Guard Maritime Intelligence Fusion Centers (MIFCs), located on each coast, receive intelligence from, and provide intelligence to, ICC. MIFCs also provide actionable intelligence to Coast Guard commanders at the district and port levels, and share that analysis with interagency partners. At the port level, Captains of the Ports (COTPs) head area maritime security committees that include federal and nonfederal stakeholders and help facilitate information sharing. Field Intelligence Support Teams (FISTs), also located at the port level, are composed of intelligence specialists who collect, analyze, and disseminate critical maritime threat information. FISTs can be colocated at interagency operational centers or Coast Guard district or sector command centers.
U.S. Customs and Border Protection (CBP)	The CBP Office of Intelligence collects, develops, analyzes, and disseminates intelligence in support of tactical and operational maritime security mission requirements and prepares strategic analysis for key decision makers. Analytical reports are prepared for DHS to disseminate to appropriate agency components and other federal agencies. CBP’s National Targeting Center (NTC) conducts “sweep” operations of information on air, sea, and land passengers, conveyances, and cargo. The center does 24-hour tactical targeting that coordinates CBP’s field operations response to terrorist threats and national security concerns, develops raw intelligence into actionable targets, and works as a liaison between other CBP offices and other federal agencies such as the Coast Guard.	CBP Advanced Targeting Units (ATUs), at the port level, screen incoming cargo that poses a possible threat to the national security of the United States.

**Appendix III: Port-Level Information Sharing
Is Supported by, and Supports, National-Level
Intelligence Infrastructure**

Department and agency/component	National-level intelligence organizations	Regional or field-level intelligence organizations
U.S. Immigration and Customs Enforcement (ICE)	ICE Office of Intelligence evaluates, disseminates, and coordinates classified intelligence community and law enforcement reporting. A central component of the ICE information-sharing effort is ICE Intelligence Watch, which evaluates all tactical intelligence of terrorist threats to the homeland and provides additional analytical support through crosschecks of all agency and intelligence community databases.	ICE has six Field Intelligence Units (FIUs) that provide geographic and regional intelligence analysis and supervise Intelligence Collection and Analysis Teams (ICATs) that are also active in the field. In the maritime domain, ICE maintains Watchtower, which is a field maritime intelligence operation that provides detailed information on incoming vessels resulting from targeted inspections of vessels and cargo. Over 20 Watchtower specialists, located at 17 seaports nationwide, produce Field Intelligence Reports (FIRs) covering all domestic seaports. Watchtower specialists meet and work with state and local law enforcement, Coast Guard, CBP, and DOJ officials. Among other things, these specialists provide information on ships (e.g., container cargo ships, tankers, and bulk carriers) that may require an enforcement action, such as a boarding or interview of the vessel master.
Transportation Security Administration (TSA)	As part of its mission to protect the nation's transportation system, TSA is tasked to develop a maritime information system in accordance with requirements of the Maritime Transportation Security Act of 2002. As such, DHS is exploring the most appropriate means of fulfilling this legislative requirement. The TSA Transportation Security Intelligence Service (TSIS) disseminates intelligence and law enforcement information about threats to transportation security and serves as a liaison for transportation security to the intelligence community. In this capacity, TSIS helps to coordinate domestic and international transportation security activities with DHS and other government agencies.	No domestic presence at the regional or field levels specifically related to maritime security.
Information Analysis and Infrastructure Protection (IAIP)	The mission of IAIP is to identify and assess current and future threats to the homeland, map those threats against known vulnerabilities, develop protective measures, issue timely warnings, and take preventive and protective action. This threat information includes, but is not limited to, the maritime environment. As part of this mission, IAIP is to provide information to federal, state, local, tribal government, law enforcement, and private sector officials as appropriate, both classified and unclassified, and also conducts a daily Information Analysis Morning Executive Brief, whereby DHS components share and coordinate threat information.	No domestic presence at the regional or field levels specifically related to maritime security.

**Appendix III: Port-Level Information Sharing
Is Supported by, and Supports, National-Level
Intelligence Infrastructure**

Department and agency/component	National-level intelligence organizations	Regional or field-level intelligence organizations
Department of Justice		
U.S. Attorneys' Offices	Executive Office for U.S. Attorneys (EOUSA) provides for close liaison between DOJ in Washington, D.C., and the 94 U.S. Attorneys' offices located throughout the nation, as well as direction, oversight, and support.	DOJ, through U.S. Attorney Anti-Terrorism Advisory Councils (ATACs), has established state and regional task forces and coordination centers that may include a maritime component or nexus, such as the Maryland Coordination and Analysis Center (MCAC).
Federal Bureau of Investigation (FBI)	Counterterrorism Division (CTD) is colocated with the National Counterterrorism Center, but remains under the direction of FBI. CTD conducts analysis, evidence exploitation, and the preparation and dissemination of finished intelligence products and briefing materials related to counterterrorism. National Joint Terrorism Task Force (NJTTF) includes representatives from the Departments of Homeland Security, Defense, Justice, Treasury, Transportation, Commerce, Energy, State, and Interior; and collects terrorism information and intelligence and funnels it to Joint Terrorism Task Forces (JTTFs).	Joint Terrorism Task Forces are multi-agency investigative teams composed of federal, state and local agencies that work jointly with other nonmember agencies to investigate terrorism matters. JTTFs are designated conduits of information from federal to state and local officials (and the private sector) and are located in 66 field offices across the country. In addition, the FBI Maritime Liaison Agent (MLA) Program is intended to enhance the security of the U.S. maritime environment by training special agents and Joint Terrorism Task Force officers serving at various port area on subjects pertaining to preventing terrorism at our nation's seaports. Designated MLAs throughout the nation are required to increase interaction between law enforcement and the private sector, state and local port authorities, and other federal agencies with maritime responsibilities.
Department of Defense		
Department of the Navy	The Office of Naval Intelligence (ONI) provides national-level maritime intelligence on merchant and non-merchant ship activity to determine possible terrorist threats abroad and at home. ONI is colocated with the Coast Guard ICC at NMIC. Naval Criminal Investigative Service (NCIS) is the primary law enforcement and counterintelligence arm of the Navy. The NCIS Multiple Threat Alert Center (MTAC) tracks worldwide threats against navy facilities and vessels.	ONI has no domestic presence at the regional or field levels specifically related to domestic maritime security. NCIS has regional agents who work closely with federal, state, and local agencies to counter terrorism and protect navy facilities and vessels, as well as shipping military equipment.
Other Intelligence Community		
Central Intelligence Agency (CIA)	CIA's Counterterrorism Center (CTC), colocated at the National Counterterrorism Center, assists CIA in coordinating the counterterrorist efforts of the intelligence community by implementing a counterterrorist operations program to collect intelligence on international terrorist groups, producing analyses of the groups and states responsible for international terrorism and coordinating the counterterrorist activities of the intelligence community. CTC has dedicated analysts to the threat against U.S. seaports and maritime assets.	No domestic presence at the regional or field levels specifically related to maritime security.

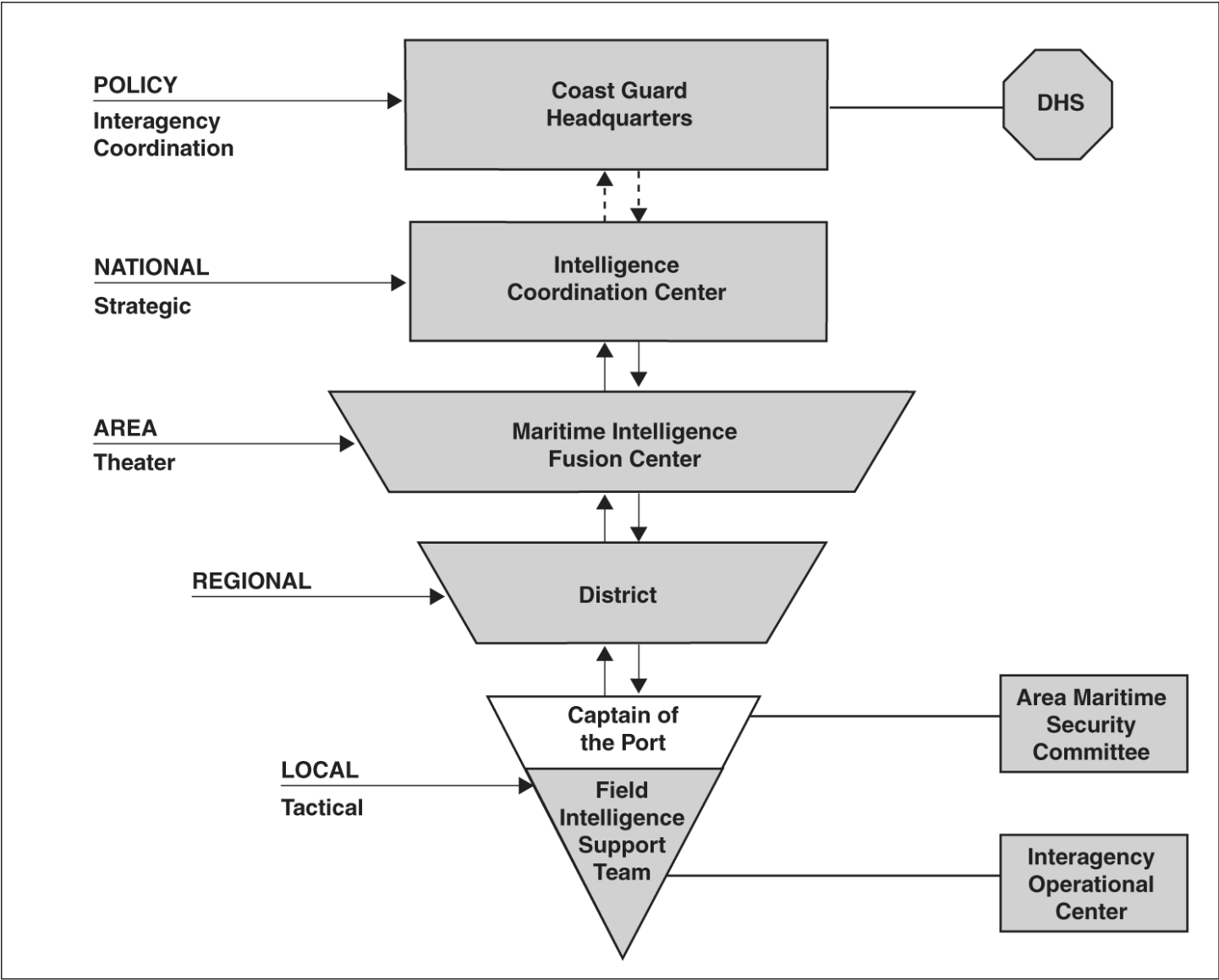
**Appendix III: Port-Level Information Sharing
Is Supported by, and Supports, National-Level
Intelligence Infrastructure**

Department and agency/component	National-level intelligence organizations	Regional or field-level intelligence organizations
National Counterterrorism Center (NCTC)	NCTC is responsible for analyzing and integrating foreign and domestic intelligence acquired from all U.S. government departments and agencies pertaining to terrorism. The center will identify, coordinate, and prioritize the counterterrorism intelligence requirements of the nation's intelligence agencies.	No domestic presence at the regional or field levels specifically related to maritime security.

Source: GAO.

The Coast Guard, as the lead in domestic maritime security, plays a central role in maritime threat information sharing and has a robust presence at the national, regional, and port levels. In this capacity, it conducts intelligence activities in support of all its missions, maritime homeland security, and national security objectives, including information collection, analysis, and dissemination of intelligence information. Figure 4 illustrates how Coast Guard national and regional maritime information is channeled to and from representatives of a local area maritime security committee (AMSC) or interagency operational center.

Figure 4: Flow of Information from National and Regional Coast Guard Sources to Area Maritime Security Committees and Interagency Operational Centers at the Port Level



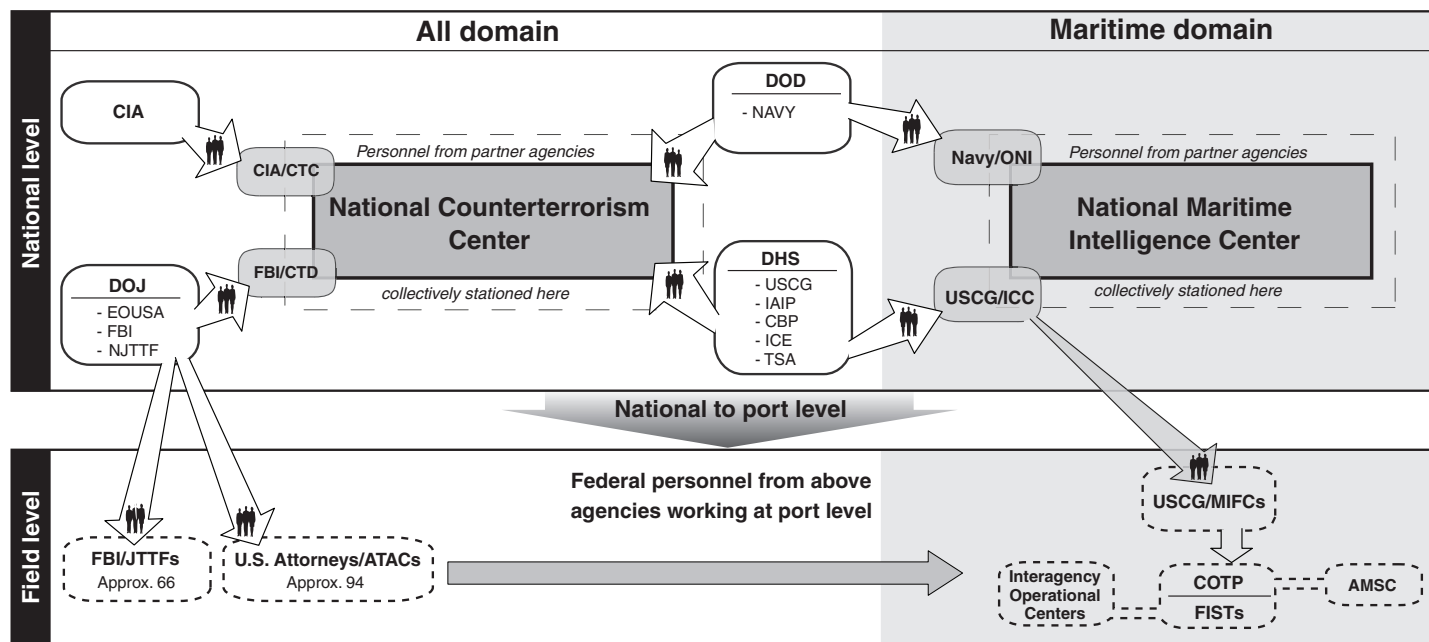
Source: GAO analysis of Coast Guard data.

Beyond the Coast Guard, other agencies can also play a major role in channeling maritime security information to the port level. As shown in table 2, some of these agencies have broader responsibilities for intelligence across all domains. For example, DOJ has a number of

organizations involved in terrorist threat information sharing, such as the National Joint Terrorism Task Force, which act as a liaison and conduit for “all domain” (e.g., maritime and nonmaritime) information from FBI headquarters to Joint Terrorism Task Forces operating in the field. The FBI also has designated Maritime Liaison Agents at the port level who interact with state, local, and private sector officials and other federal agencies, to enhance security at the nation’s seaports. In addition, U.S. Attorneys’ Offices of DOJ set up Anti-terrorism Advisory Councils that sponsor state- or regional-level task forces or coordination centers that may include a maritime security component. Figure 5 graphically illustrates (1) how maritime and nonmaritime information and intelligence is shared among agencies at the national level and (2) organizational conduits through which information is shared with the port level. The left side of the figure shows DOJ channels for information discussed above. On the right side, the figure also shows the flow of information through Coast Guard channels, as already shown in figure 4.

Appendix III: Port-Level Information Sharing
Is Supported by, and Supports, National-Level
Intelligence Infrastructure

Figure 5: Flow of Information between National Intelligence and Law Enforcement Agencies and between the National and the Port Level



Source: GAO.

Appendix IV: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

April 5, 2005

Ms. Margaret T. Wrightson
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Wrightson:

RE: Draft Report GAO-05-394, New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention (GAO Job Code 440283)

The Department of Homeland Security (DHS), including the Coast Guard, appreciates the opportunity to comment on the Government Accountability Office's draft report.

We generally agree with the findings and recommendations made. The report notes that Coast Guard has lead responsibility in coordinating maritime information sharing efforts to secure the nation's ports against potential terrorist attack. Coast Guard established area maritime security committees and, working with other agencies including other DHS components, has further enhanced information sharing and port security operations by establishing interagency operational centers. Both the area maritime security committee structure and the interagency operational centers have resulted in greater information sharing among interested federal, state, and local governments, and the private sector.

Recommendations intended to improve information sharing among nonfederal officials should enhance Coast Guard's on-going efforts promoting information sharing among port security stakeholders. Changes associated with processing security clearances should overcome identified impediments to otherwise successful attempts to strengthen port security through the involvement of various stakeholders. As mentioned in the draft, Coast Guard officials are taking steps to provide guidance to field office personnel to improve information sharing.

GAO also acknowledges the role of other DHS components in promoting information sharing. For example, Customs and Border Protection (CBP) officials may be members of area maritime security committees thereby lending their expertise in an effort to promote security. In addition, the interagency operational center in Charleston, South Carolina includes the Department of Justice as well as DHS' CBP, Immigration and Customs Enforcement (ICE), and Coast Guard. The report notes that representatives

www.dhs.gov

**Appendix IV: Comments from the Department
of Homeland Security**

from the various agencies and DHS' components work side by side, each having access to databases and other sources of information from their respective agencies. For example, the Charleston center has access to both Coast Guard technology systems and various national databases in addition to CBP's databases on incoming cargo containers.

Coast Guard, other DHS components, other federal agencies, state and local governments, and the private sector are sharing information. More can be done, but progress has been made.

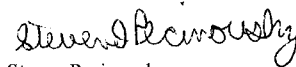
We also appreciate the recognition of the DHS Homeland Security Task Force, South-East. This interagency arrangement is in addition to the interagency operational centers and consists of federal and nonfederal agencies that have the mission to respond to mass migration of immigrants affecting the south eastern United States. This task force was activated in 2004 to interdict a mass migration from Haiti.

The report discusses another example of an interagency arrangement for information sharing wherein single-agency operational centers can become interagency. As mentioned, Coast Guard has its own command centers that normally focus on a variety of Coast Guard missions and that are not normally interagency in structure. However, Coast Guard has established protocols with DHS components, CBP and ICE, to activate a unified or incident command structure should one be needed to respond to specific events. These types of interagency arrangements often include various DHS components and are crucial to sharing information and coordinating operations.

Since the release of the draft report, the Coast Guard report required by Congress relating to existing interagency operational centers has been approved by DHS and the Office of Management and Budget. The report is now in the final stages of review at Coast Guard.

We are providing technical comments to your office under separate cover.

Sincerely,



Steven Pecinovsky
Director
Departmental GAO/OIG Liaison Office

MMcP

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Margaret T. Wrightson (415) 904-2200
Stephen L. Caldwell (202) 512-9610

Staff Acknowledgments

In addition to those named above, David Alexander, Neil Asaba, Juliana Bahus, Christine Davis, Kevin Heinz, Emily Pickrell, Albert Schmidt, Amy Sheller, Stan Stenersen, and April Thompson made key contributions to this report.

Related GAO Products

Coast Guard: Observations on Agency Priorities in Fiscal Year 2006 Budget Request. [GAO-05-364T](#). Washington, D.C.: March 17, 2005.

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

Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program. [GAO-05-106](#). Washington, D.C.: December 10, 2004.

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

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

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

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

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

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

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

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

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

Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened. [GAO-03-760](#). Washington D.C.: August 27, 2003.

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

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

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

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

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

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

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

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

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

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

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