United States Government Accountability Office

GAO

Testimony before the Subcommittee on Government Management, Finance, and Accountability, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 1:00 p.m. EDT
Monday, July 10, 2006

MARITIME SECURITY

Information-Sharing Efforts Are Improving

Statement of Stephen L. Caldwell, Acting Director
Homeland Security and Justice Issues

GAO
Accountability * Integrity * Reliability

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-933T, a testimony before the Subcommittee on Government Management, Finance, and Accountability of the Committee on Government Reform, U.S. House of Representatives

July 10, 2006

MARITIME SECURITY

Information-Sharing Efforts Are Improving

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.

This testimony is a summary and update to our April 2005 report, *Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention*, GAO-05-394. It discusses the impact the committees and interagency operational centers have had on improving information sharing and identifies any barriers that have hindered information sharing.

www.gao.gov/cgi-bin/getrpt?GAO-06-933T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Stephen L. Caldwell at (202) 512-9610 or CaldwellS@gao.gov.

What GAO Found

Area maritime security committees provide a structure that has improved 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. GAO's ongoing work indicates that these committees continue to be useful forums for information sharing.

Interagency operational centers also 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 has developed its own centers—called sector command centers—at 35 port locations to monitor information and to support its operations planned for the future. As of today, the relationship between the interagency operational centers and the sector command centers remains to be determined.

In April 2005 the major barrier hindering information sharing was the lack of federal security clearances for nonfederal members of committees or centers. In April 2005, Coast Guard issued guidance to field offices that clarified their role in obtaining clearances for nonfederal members of committees or centers. In addition, the Coast Guard did not have formal procedures that called for the use of data to monitor application trends. As of June 2006, guidance was put in place and according to the Coast Guard, was responsible for an increase in security clearance applications under consideration by the Coast Guard. Specifically, as of June 2006, 188 out of 467 nonfederal members of area maritime security committees with a need to know received some type of security clearance. This is an improvement from February 2005, when no security clearances were issued to 359 nonfederal members of area maritime security committees members with a need to know security information.

Harbor Patrols Coordinated by Interagency Operational Centers

Source: GAO.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the improvements made in the practice of sharing maritime-related security information. 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, their inclusion of critical infrastructures such as oil refineries and terminals, and their importance to the nation's economy and trade. Although no port-related terrorist attacks have occurred in the United States, terrorists overseas have demonstrated their ability to access and destroy infrastructure, assets, and lives in and around seaports.

Ports are sprawling enterprises that often cross jurisdictional boundaries; therefore, the need to share information among federal, state, and local agencies is central to effective prevention and response. Since the September 11 terrorist attacks, the federal government has taken a number of approaches designed to enhance information sharing.[1] One of these approaches provides the Coast Guard with the authority to create area maritime security committees at the port level.[2] These committees—with representatives from the federal, state, local, and private sectors—offer a venue to identify and deal with vulnerabilities in and around ports, as well as a forum for sharing information on issues related to port security. Another approach developed to share information is the creation of interagency operational centers at certain port locations.[3] These centers are command posts that tie together intelligence and operational efforts of various federal and nonfederal participants. Often information regarding

[1] For the purposes of this testimony, "homeland security information sharing" is defined as an exchange of information, including intelligence, critical infrastructure, and law enforcement information, among federal, state, and local governments, and the private sector (industry) to establish timely, effective, and useful communications to detect, prevent, and mitigate potential terrorist attacks.

[2] The Maritime Transportation Security Act of 2002 (MTSA), 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.

[3] We 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. Members of these interagency operational centers include the Department of Homeland Security (through the U.S. Coast Guard), the Department of the Navy, and the Department of Justice.

port security is classified, and requires security clearances for those who need access to this information. Lacking access to such information through a security clearance can disadvantage officials in their efforts to respond to or combat a terrorist threat.

My testimony today is a summary of and update to our April 2005 report, *Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention*, GAO-05-394. That report provides additional background and examples related to our findings. Specifically, my testimony provides an examination of the efforts that the Coast Guard and other federal agencies have made in improving information sharing among federal, state, local, and industry stakeholders, including (1) the impact of area maritime security committees on information sharing, (2) the impact of interagency operational centers on information sharing, and (3) the barriers, if any, that have hindered improvements in information sharing among port security stakeholders.

To obtain this information, we reviewed the activities of area maritime security committees at four ports, selected to provide a diverse sample of security environments and perspectives. The ports were Baltimore, Maryland; Charleston, South Carolina; Houston, Texas; and Seattle, Washington. To review the activities of the interagency operational centers, we visited and interviewed participants at the three centers in operation at the time of our published report. We also discussed information-sharing issues with nonfederal stakeholders, including private sector officials, officials from port authorities, and local law enforcement. We examined the Coast Guard's procedures for processing security clearances for members of area maritime security committees. We reviewed legislation and congressional committee reports related to information sharing, interviewed agency officials, and reviewed numerous other documents and reports on the issue. We interviewed Coast Guard officials involved in sharing information and received updated information about their efforts in 2006. All of our work has been conducted in accordance with generally accepted government auditing standards.

Summary

Judging from the four ports we visited for our 2005 report, area maritime security committees have provided a structure to improve the timeliness, completeness, and usefulness of information sharing between federal and nonfederal stakeholders. Stakeholders said the newly formed committees were an improvement over previous information-sharing efforts because they 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 locations we visited had the same guidance, they varied in such ways as the size of the membership and the types of stakeholders represented.

The three interagency operational centers we visited for our 2005 report 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 operational interagency centers and two additional centers under construction should 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 the Department of Justice (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 also has developed its own operational centers—called sector command centers—at 35 port locations, including four sector command centers with enhanced surveillance and collaboration capabilities,[4] to monitor maritime information and to support Coast Guard operations.

[4] The four sector command centers with enhanced surveillance and collaboration capabilities are Miami, Florida; San Diego, California; Charleston, South Carolina; and Hampton Roads, Virginia. The Coast Guard told us that the long-term goal is to provide all sector command centers with enhanced surveillance and collaboration capabilities.

One barrier to sharing information—the lack of security clearances among nonfederal officials—is being addressed by the Coast Guard. In our April 2005 report, we noted that while information sharing has generally improved, a major barrier mentioned most frequently by stakeholders as hindering information sharing was the lack of federal security clearances among port security stakeholders. This 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 359 nonfederal area maritime security committee participants as having a need for a security clearance—only 28 had submitted the necessary paperwork for the background check**.** As of June 2006, Coast Guard identified 467 nonfederal area maritime security committee participants with a need to know security information. Of the 467 nonfederal participants, 197 security clearance applications were received—20 received interim clearances, and 168 received final security clearances. Therefore, according to the Coast Guard, 188 out of 467 area maritime security committee participants with a need to know have received some type of clearance. Although we reported in 2005 that progress in moving these officials through the application process had been slow, it appears that as of June 2006, the Coast Guard's efforts have improved considerably. However, continued management attention and guidance about the security clearance process would strengthen the program, and it would reduce the risk that nonfederal officials may have incomplete information as they carry out their law enforcement activities.

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 cargo containers, and bulk agricultural, mineral, petroleum, and paper products. Ports are also important to national security by hosting naval bases and vessels and facilitating the movement of military equipment and supplying troops deployed overseas.

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 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

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. 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

Information sharing among federal, state, and local officials is central to port security activities. The Homeland Security Act of 2002 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.[5]

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. 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.[6] To obtain a

[5] P.L. 107-296, § 891 (Nov. 25, 2002).

[6] Executive Order 12968, Access to Classified Information, Section 1.1(h).

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.

Area Maritime Security Committees

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—composed of federal, state, local, and industry members—to be established by the Coast Guard at ports across the country.[7] 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.[8] The committees also serve as a link for communicating threats and disseminating security information to port stakeholders. As of June 2006, the Coast Guard organized 46 area maritime security committees, covering the nation's 361 ports.[9]

Interagency Operational Centers

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 are to 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. These interagency operational centers represent 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

[7] See 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.

[8] See 33 C.F.R. § 103.500.

[9] Because 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.

vessels, aircraft, and other vehicles and stations involved in port security operations.

Port-Level Information Sharing Supported by National-Level Intelligence

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.[10]

Area Maritime Security Committees Have Improved Information Sharing

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. 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. 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. Also, participants noted that these committees allowed for both formal and

[10] For a more detailed description of the departments and agencies/components involved in maritime information sharing at the national and port levels, see appendix II of *Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention.* GAO-05-394, (Washington, D.C.: Apr. 15, 2005).

informal stakeholder networking, which contributes to improvements in information sharing.

Our continuing work on the Coast Guard and maritime security, while not specifically focused on information sharing, has continued to indicate that area maritime security committees are a useful tool for exchanging information. For example, we have done work at eight additional ports and found that stakeholders were still using the committees as a structured means to regularly share information about threat conditions and operational issues. In addition, Coast Guard personnel and port stakeholders are using the area maritime security committees to coordinate security and response training and exercises. Also, in the wake of Hurricane Katrina, Coast Guard officials shared information collaboratively through their area maritime security committees to determine when it was appropriate to close and then reopen a port for commerce.

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.

Interagency Operational Centers Have Also Improved Information Sharing

Centers Process and Share Information on Operations

Information sharing at interagency operational centers represents a step toward further improving information sharing, according to participants at the centers we visited. They said 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 a continuous flow of 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 and include data on vessels, cargo, and crew.

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. At the centers we visited, representatives from the various agencies work side by side, each having access to databases and other sources of information from their respective agencies. Officials said such centers help leverage the resources and authorities of the respective agencies. For example, if the Coast Guard determines that a vessel should be boarded and inspected, 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.

Variations across Centers Affect Information Sharing

The types of information and the way information is shared vary at the centers we visited, depending on their purpose and mission, leadership and organization, membership, technology, and resources, according to officials at the centers. In our report of April 2005, we detailed three interagency operational centers at Charleston, South Carolina; Norfolk, Virginia; and San Diego, California. As of June 2006, the Coast Guard has two additional interagency command centers under construction in Jacksonville, Florida, and Seattle, Washington. Both are being established as Sector Command Centers—joint with the U.S. Navy—and are expected to be operational in 2006.

Of the interagency centers we visited, the Charleston center had a port security purpose, so its missions were all security related. It was led by DOJ, and its membership included 4 federal agencies and 16 state and local agencies. The San Diego center had a more general purpose, so it had multiple missions to include not just port security, but search and rescue, environmental response, drug interdiction, and other law enforcement activities. It was led by the Coast Guard, and its membership included 2 federal agencies and 1 local agency. The Norfolk center had a port security purpose, but its mission was focused primarily on force protection for the Navy. It was led by the Coast Guard, and its membership included 2 federal agencies and no state or local agencies. As a result, the Charleston center shared information that focused 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 shared information on a broader scope of activities (beyond security) among a smaller group of federal and local agency officials. The Norfolk center shared the most focused information (security information related to force protection) among two federal agencies.

The centers also shared different information because of their technologies and resources. The San Diego and Norfolk centers had an array of standard and new Coast Guard technology systems and access to Coast Guard and various national databases, while the Charleston center had these as well as additional systems and databases. For example, the Charleston center had access to and shared information on Customs and Border Protection's databases on incoming cargo containers from the National Targeting Center. In addition, Charleston had a pilot project with the Department of Energy to test radiation detection technology that provided additional information to share. The Charleston center was funded by a special appropriation that allowed it to use federal funds to pay for state and local agency salaries. This arrangement boosted 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 had 24-hour participation by the local harbor patrol, that agency was paying its own salaries.

Coast Guard Continues to Develop Sector Command Centers at Ports

In April 2005, we reported that the Coast Guard planned to develop up to 40 of its own operational centers—called sector command centers—at additional ports. These command centers would provide local port activities with a unified command and improve awareness of the maritime domain through a variety of technologies. As of June 2006, the Coast Guard reported to us that 35 sector command centers have been created, and that these centers are the primary conduit for daily collaboration and coordination between the Coast Guard and its port partner agencies. The Coast Guard also reported that it has implemented a maritime monitoring system—known as the Common Operating Picture system—that fuses data from different sources.[11] According to the Coast Guard, this system is the primary tool for Coast Guard commanders in the field to attain maritime domain awareness.

In April 2005, we also reported that the Coast Guard requested in fiscal year 2006 over $5 million in funding to improve awareness of the maritime domain by continuing to evaluate the potential expansion of sector command centers to other port locations, and requested additional funding to train personnel in Common Operating Picture deployment at command centers and to modify facilities to implement the picture in command centers.[12] In June 2006, the Coast Guard reported to us that no additional funding for this program was requested for fiscal year 2007.

Coast Guard Report on Interagency Operational Centers

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.[13] This report, called for by February 2005, was issued by the Coast Guard in April 2005. While the report addresses the information sought by Congress, the report did not define the relationship between interagency operational centers and the Coast Guard's own sector command centers.

Port stakeholders reported to us 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

[11] The Coast Guard reported to us that some of the data systems included in its maritime monitoring system include data from the Department of Defense, Shipboard Command and Control System; data from Integrated Deepwater Systems; imagery from aircraft; data from Vessel Traffic Service, Ports and Waterways Safety Stems, Joint Harbor Operations Commands, Automated Identification Systems, Inland Rivers Vessel Movement Center, and the Vessel Monitoring System. However, according to the Coast Guard, not all of these data are available to all units; full integration is a future goal of the Coast Guard.

[12] 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.

[13]See *t*he 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.

purposes, as well as support a wide number of specific missions; (2) leadership and organization—the centers could be led by several potential 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.

Other Ad Hoc Arrangements for Interagency Information-Sharing

Our work 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. 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 a contingency plan.

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 District Seven and Sector Miami, located in Miami, Florida. 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 the U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, to activate a unified or incident command structure should it be needed. 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.

Interagency Information-Sharing Concerns Go Beyond Maritime Area

While our findings on maritime information sharing are generally positive, we have some concerns regarding interagency information sharing that go far beyond the maritime issue area. 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 disseminating key information within and among federal and nonfederal entities.[14] While we recognize the efforts that some agencies have undertaken to break out of information “silos” and better share information, we reported in 2006 that more than 4 years after September 11, the nation still lacks comprehensive policies and processes to improve the sharing of information that is critical to protecting our homeland.[15] We made several recommendations to the Director of National Intelligence, who is now primarily responsible for this effort, to ensure effective implementation of congressional information sharing mandates.

We continue to review agencies and programs that have the goal of improving information sharing among federal, state, and local partners. For example, we have ongoing work assessing DHS’ efforts to enhance coordination and collaboration among interagency operations centers that operate around the clock to provide situational awareness. We plan to report on this later this year. Also, we have just begun work on state fusion centers--which are locations where homeland security-related information can be collected and analyzed--and their links to their relevant federal counterparts, which we plan to report on in 2007.

Coast Guard Making Progress Granting Security Clearances

Lack of Security Clearances May Limit Ability to Confront Terrorist Threats

According to the Coast Guard and state and local officials we contacted for our 2005 report, 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 lack of

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

[15] GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: March 2006).

access to classified information may limit these officials' 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 2005 report, 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 Continues to Take Steps to Grant Additional Clearances to State, Local, and Industry Officials

In April 2005, we reported that 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. We also reported that as of February 2005, only 28 of 359 nonfederal committee members who had a need to know had submitted the application forms for a security clearance. As shown in table 1, as of June 2006, of the 467 nonfederal committee members who had a need to know, 197 had submitted security clearance applications—20 received interim clearances, and 168 were granted a final clearance, which allows access to classified material.

Table 1: Comparison of February 2005 Coast Guard Data Regarding Security Clearances and June 2006 Coast Guard Data Regarding Security Clearances

Security clearance totals	February 2005	June 2006
Nonfederal committee members verified as needing clearances	359	467
Members who had submitted security clearance case paperwork	28 (8 percent of 359)	197 (42 percent of 467)
Members granted interim clearances pending final investigations from Office of Personnel Management	24 (7 percent of 359)	20 (4 percent of 467)
Members with final clearances at Secret level	0 (0 percent of 359)	168 (36 percent of 467)

Source: Coast Guard.

Data Are Being Used to More Effectively 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. We reported in April 2005 that the Coast Guard was testing the database for use by field staff, but had not granted field staff access to the database. As of June 2006, the Coast Guard granted access to this database—named Checkmate—to field staff. The second database—an internally developed spreadsheet on the area maritime committee participants—summarizes information on the status of the security clearance program, such as whether officials have submitted their application forms and whether they have received their clearances.

We reported in 2005 that these Coast Guard has databases could be used to manage the state, local, and industry security clearance program, but that 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 had not been developed by the Coast Guard. While it is unclear that the Coast Guard developed formal procedures, as of June 2006, the Coast Guard reported that it has developed guidance for using its data on committee participants. According to the Coast Guard, the guidance released to field commands regarding the state, local, and industry security clearance program clarified the process for nonfederal area maritime security committee members to receive clearances and specifically outlined responsibilities for working with applicants on completing required paperwork, including the application packages. The Coast Guard reported that as a result of this guidance, the number of received and processed security clearance packages for area maritime security committee members has increased.

Concluding Observations

As we reported in April 2005, and reaffirm today, 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, and although we reported in 2005 that progress in moving these officials through the application process had been slow, it appears that as of June 2006 the Coast Guard's efforts to process security clearances to nonfederal officials has improved considerably. However, continued management attention and guidance about the security clearance process would strengthen the program, and it would reduce the risk that nonfederal officials may have incomplete information as they carry out their law enforcement activities.

Mr. Chairman and members of the subcommittee, this completes my prepared statement. I would be happy to respond to any questions that you or other members of the subcommittee may have at this time.

GAO Contacts and Staff Acknowledgments

For information about this testimony, please contact Stephen L. Caldwell Acting Director, Homeland Security and Justice Issues, at (202) 512-9610, or at caldwells@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found at the last page of this statement. Individuals making key contributions to this testimony include Susan Quinlan, David Alexander, Neil Asaba, Juliana Bahus, Christine Davis, Kevin Heinz, Lori Kmetz, Emily Pickrell, Albert Schmidt, Amy Sheller, Stan Stenersen, and April Thompson.

Related GAO Products

Coast Guard: Observations on Agency Performance, Operations, and Future Challenges. GAO-06-448T. Washington, D.C.: June 15, 2006.

Maritime Security: Enhancements Made, but Implementation and Sustainability Remain Key Challenges. GAO-05-448T. Washington, D.C.: May 17, 2005.

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

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

Coast Guard: Station Readiness Improving, but Resource Challenges and Management Concerns Remain. GAO-05-161. Washington, D.C.: January 31, 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.

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.

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

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.

(440531)

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