United States General Accounting Office

GAO

Report to the Chairman, Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, House of Representatives

October 2002

COMBATING TERRORISM

Actions Needed to Improve Force Protection for DOD Deployments through Domestic Seaports

GAO-03-15

Contents

Tables

Figures

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

October 22, 2002

The Honorable Christopher Shays
Chairman, Subcommittee on National Security, Veterans Affairs,
and International Relations
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

The October 12, 2000, attack against the Navy destroyer U.S.S. *Cole* in the port of Aden illustrated the danger of unconventional threats to U.S. ships in seaports. The September 11 attacks further heightened the need for a significant change in conventional antiterrorist thinking, particularly regarding threats to the U.S. homeland. The new security paradigm assumes that all U.S. forces, be they abroad or at home, are vulnerable to attack, and that even those infrastructures traditionally considered of little interest to terrorists, such as commercial seaports in the continental United States, are now commonly recognized as highly vulnerable to potential terrorist attack. The Department of Defense (DOD) and all agencies associated with seaport security recognize this new paradigm and are taking steps to reduce vulnerabilities and increase security.

Of the more than 300 seaports in the United States, the Departments of Defense and Transportation have designated 17 as "strategic," because in the event of a large-scale military deployment, DOD would transport more than 95 percent of all equipment and supplies needed for military operations by sea. These ports are therefore vital to national security. If the strategic ports (or the ships carrying military supplies) were attacked, not only could massive civilian casualties be sustained, but DOD could also lose precious cargo and time and be forced to rely heavily on its overburdened airlift capabilities.

Military commanders are responsible for the protection of personnel, equipment, and other assets. To achieve this objective, commanders apply a "risk management" approach, which is a systematic, analytical process to determine the likelihood that a threat will negatively impact physical assets, individuals, or operations and identify actions to reduce risk and mitigate the consequences of an attack. The principles of risk management acknowledge that although risk generally cannot be eliminated, it can be significantly reduced by enhancing protection from known or potential threats.

You asked us to examine how DOD protects its forces and assets as it deploys them through strategic commercial seaports. This report focuses on domestic seaports and analyzes (1) the security environment at domestic strategic seaports used by DOD for military deployments and (2) DOD's process for securing military deployments through those ports. Overseas seaports will be the focus of a subsequent review.

As part of our evaluation, we examined seaport force protection efforts at six strategic seaports in the United States. Although the information we obtained at these locations cannot be generalized to describe DOD's overall seaport force protection, it provides insight into how force protection efforts at strategic seaports were implemented at selected locations. For security reasons, we do not discuss location-specific information in this report. Further information on our scope and methodology appears in appendix I.

Results in Brief

The security environment at strategic seaports remains uncertain because comprehensive assessments of threats, vulnerabilities, and critical port infrastructure and functions have not been completed, and no effective mechanism exists to coordinate and disseminate threat information at the seaports. These conditions compound the already difficult task of protecting deploying forces and increase the risk that threats—both traditional and nontraditional[1] ones—may not be recognized or that threat information may not be communicated in a timely manner to all relevant organizations. Recent efforts by the Coast Guard, the Transportation Security Administration, and other agencies at the ports have begun to address many of these weaknesses. The Coast Guard initiated vulnerability assessments of port infrastructure and is deploying additional teams dedicated to seaport security. Further, if enacted, legislation currently before the Congress proposes steps that may assist these efforts and provides additional measures that could improve the coordination and dissemination of threat information.

We identified two significant weaknesses in DOD's force protection process for deployments through domestic seaports. First, DOD lacks a central authority responsible for overseeing force protection measures of DOD organizations that move forces from domestic installations through

[1] Nontraditional threats can include natural or man-made disasters, such as hurricanes, industrial accidents, and cyber attacks.

U.S. seaports. As a result, potential force protection gaps and weaknesses requiring attention and action might be overlooked. DOD has such an authority for the overseas portions of deployments and is therefore better able to identify and mitigate force protection gaps there. Second, during some phases of a deployment, DOD transfers custody of its military equipment to non-DOD entities, including foreign-owned ships crewed by non-U.S. citizens. Although consistent with current DOD policies and procedures, this practice limits DOD's ability to provide security oversight. As a result, equipment could fall into the hands of individuals or groups whose interests are counter to those of the United States.

We are making recommendations to improve (1) threat information coordination at strategic seaports, (2) DOD's oversight and coordination of force protection for deployments through seaports, and (3) DOD's control over the in-transit phases of a movement of equipment. In comments on a draft of this report, the Departments of Defense and Transportation generally agreed with the contents of this report and its recommendations.

Background

DOD defines force protection as "actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information."[2] Our review concentrated mostly on the physical security and related aspects of force protection that include measures to protect personnel and property and encompass consequence management, intelligence, and critical infrastructure protection.

We have identified a risk management approach used by DOD to defend against terrorism that also has relevance for the organizations responsible for security at commercial seaports. This approach can provide a process to enhance preparedness to respond to terrorist attacks or other emergencies, whether natural or man-made (intentional or unintentional). The approach is based on assessing threats, vulnerabilities, and criticalities (the importance of critical infrastructure and functions).

Threat assessments identify and evaluate potential threats on the basis of factors such as capabilities, intentions, and past activities. These assessments represent a systematic approach to identifying potential

[2] Department of Defense, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Apr. 12, 2001, as amended through May 7, 2002).

threats before they materialize. However, even if updated frequently, threat assessments may not adequately capture all emerging threats. The risk management approach therefore uses vulnerability and criticality assessments as additional input to the decision-making process.

Vulnerability assessments identify weaknesses that may be exploited by identified threats and suggest options that address those weaknesses. For example, a vulnerability assessment might reveal weaknesses in a seaport's security systems, police force, computer networks, or unprotected key infrastructure such as water supplies, bridges, and tunnels. In general, teams of experts skilled in areas such as structural engineering, physical security, and other disciplines conduct these assessments.

Criticality assessments evaluate and prioritize important assets and functions in terms of factors such as mission and significance as a target. For example, certain power plants, bridges, computer networks, or population centers might be identified as important to the operation of a seaport. Criticality assessments provide a basis for identifying which assets and structures are more important to protect from attack. These assessments also help determine mission-essential requirements to better prioritize limited force protection resources while reducing the potential for expending resources on lower priority assets.

In the event of a major military mobilization and overseas deployment, such as Operation Desert Shield, a large percentage of U.S. forces (equipment and other materiel) would be sent by sea through a number of commercial seaports in the United States to their respective areas of operations. [3] To accomplish this, DOD would use several shipping methods, including government-owned and maintained reserve sealift ships[4] and ships operated or chartered by the Military Sealift Command. Figure 1 shows two reserve sealift ships berthed at a commercial seaport.

[3] Most personnel would be transported by air.

[4] These reserve ships are part of the Maritime Administration's Ready Reserve Force.

Figure 1: Reserve Sealift Ships Berthed at a Commercial Seaport

Source: GAO.

The military also uses commercial seaports for deployments such as those to operations in the Balkans. The Departments of Defense and Transportation have identified 17 seaports on the Pacific, Atlantic, and Gulf Coasts (13 commercial ports, 1 military port, and 3 military ammunition ports) as "strategic," meaning that they are necessary for use by DOD in the event of a large scale military deployment.

Because the security activities that DOD may conduct outside its installations are limited, it must work closely with a broad range of federal, state, and local agencies to ensure that adequate force protection measures exist and are executed during deployments through strategic seaports. Force protection responsibilities for DOD deployments through commercial seaports are divided among a number of DOD organizations including the U.S. Transportation Command and its components (particularly the Military Traffic Management Command and the Military Sealift Command), the U.S. Army Forces Command, and individual deploying units.

Port Readiness Committees[5] at each strategic port provide a common coordination structure for DOD, the Coast Guard, and other federal, state, and local agencies at the port level and are the principal interface between DOD and other officials at the ports during the movement of military equipment. The Port Readiness Committees are focused largely on preparing for potential military movements through a port and not on day-to-day security concerns at the port.

The issue of security at the nation's seaports has been the subject of a recent major study, as has the broader issue of homeland security. In fall 2000, the Interagency Commission on Crime and Security in U.S. Seaports reported that security at seaports needed to be improved in a number of areas, including

- assessments of threats, vulnerabilities, and critical infrastructure at ports;
- coordination and cooperation among agencies; and
- establishment of guidelines for commercial facilities handling military cargo.

In February 2001, the Commission on National Security/21st Century (commonly referred to as the Hart-Rudman Commission) reported that threats such as international terrorism would place the U.S. homeland in great danger. In addition to recommending national action, the commission urged DOD to pay closer attention to operations within the United States.

Current Risk Management Approach Creates Uncertainties about the Security Environment at Strategic Seaports

The security environment at strategic seaports is uncertain because comprehensive assessments of threats, vulnerabilities, and port infrastructure and functions have not been completed. Recent efforts by the Coast Guard, the Transportation Security Administration, and other agencies at the ports have begun to address several important security issues, and maritime security legislation before the Congress may assist these efforts. Further, proposed legislation may provide a framework for seaport organizations to improve the coordination and dissemination of threat information.

[5] The Port Readiness Committees are part of the National Port Readiness Network chaired by the Maritime Administration.

Weaknesses Exist in the Process to Assess Risk at Seaports

There is a wide range of vulnerabilities at strategic seaports, including critical infrastructure such as bridges and refineries in close proximity to open shoreline, shipping containers with unknown contents, and an enormous volume of foreign and domestic shipping traffic. Figure 2 illustrates typical commercial port infrastructure and operations.

Figure 2: A Commercial Container Vessel and Related Infrastructure at a Seaport

Source: GAO.

Many of the organizations responsible for seaport security do not have the resources (such as trained personnel, equipment, and funding) necessary to mitigate all vulnerabilities. To determine how best to allocate available resources and address security at seaports, it is vital that responsible agencies involved follow a risk management approach that includes assessments of threats, vulnerabilities, and critical infrastructure and functions. The results of these assessments should then be used to better conduct risk-based decisions involving security planning and actions.

Since September 11, the organizations responsible for security at strategic seaports have increased emphasis on security planning. They now recognize that planning must include the protection of critical seaport

infrastructure and assets that have not generally been considered vulnerable. Port authority officials stated that increased security planning has led to improvements in physical security, such as higher fences, more security personnel, and better coordination with local law enforcement and other agencies. The Coast Guard has taken broad actions forward and has redirected resources towards security planning improvements.

However, in their planning efforts, the organizations at the ports we visited applied the elements of risk management differently. At only one of six ports we visited were the results of threat, vulnerability, and criticality assessments incorporated into a seaport security plan that included all relevant agencies. The *Port Mobilization Master Plan* developed by the Port Readiness Committee at this port employs a risk-based process and systematically identifies the mission, responsibilities, and functional relationships of each activity or agency involved in supporting a military deployment through the port.[6] Specific weaknesses in the assessment process used at ports we studied include the following:

- Individual organizations at the seaports conducted separate vulnerability assessments that were not coordinated with those of other agencies and were not based on standardized approaches. The Coast Guard has taken the lead in developing a standard methodology for comprehensive portwide vulnerability assessments (also called port security assessments) that it plans to complete at 50 major ports, including all strategic seaports.
- Assessments of the criticality of seaport infrastructure were not done at all the ports we visited prior to September 11. The Coast Guard has since addressed this shortcoming by conducting assessments of high-risk infrastructure at all major ports. It coordinated the assessments with commercial facilities at the ports. Criticality of seaport assets and functions will also be incorporated into the port security assessments.
- In some cases, threat assessment information received by agencies at the ports is based on higher-level regional assessments that do not focus on the local port facility. These regional assessments, while helpful in providing a broader view of the security environment, do not provide site-specific local threat information to the port.
- Agencies involved with seaport security have different concepts of how threat assessments should be developed and the degree to which threat information should be shared and disseminated. Some agencies have not traditionally shared threat information as widely as may be necessary for

[6] The local Port Readiness Committee is currently revising the master plan.

comprehensive security measures at seaports.

In addition to these specific weaknesses, we found that there is no single mechanism (such as a working group or committee) at the seaports we visited to analyze, coordinate, and disseminate information on a routine basis on the broad range of threats at each port. Most threat information at the ports was coordinated on an informal basis, such as through personal contacts between law enforcement individuals and those at other agencies. The lack of such a mechanism compounds the already difficult task of protecting deploying military forces and increases the risk that threats—both traditional and nontraditional ones—may not be recognized or that threat information may not be communicated in a timely manner to all relevant organizations. Currently, interagency bodies at or near the ports, such as port readiness committees, joint terrorism task forces, or the newly formed antiterrorism task forces, do not routinely coordinate threat information focused solely on the ports. The port readiness committees were designed to prepare commercial ports to conduct military movements. The task forces were designed to focus on threat information but on a regional rather than a port level.

The need for efficient coordination of threat information has been amply documented and recognized, and there are examples of improved coordination efforts. The Interagency Commission on Crime and Security in U.S. Seaports noted in 2000 the importance of interagency threat coordination. The commission said that officials at seaports need a means to analyze, coordinate, and disseminate information on the broad range of threats they face. This includes information on ships, crews, and cargo and information on criminal, terrorist, and other threats with foreign and domestic origins. Although the commission did not recommend centralizing threat information distribution into a single agency or regulating dissemination procedures at seaports, it did recommend improvements in integrating threat information systems and improved coordination mechanisms for law enforcement agencies at the seaport level.

Furthermore, the Coast Guard recognizes that agencies involved with seaport security are currently unable to adequately analyze, share, and exploit available threat information, and it also recognizes that

asymmetric[7] military and terrorist threats have a natural gateway into America via its ports. In response, the Coast Guard has developed a "maritime domain awareness" concept that emphasizes a risk management approach for preventing or mitigating both traditional and nontraditional threats through the analysis and dissemination of threat information. The concept involves being knowledgeable of all activities and elements in the maritime domain that could represent threats to the safety, security, or environment of the United States or its citizens. Through the timely delivery to the appropriate civilian or military authorities of processed information, drawn from all available sources, effective actions involving limited resources can be taken. Additionally, the maritime domain awareness concept allows the Coast Guard and other relevant agencies to incorporate nontraditional threat information, such as unintentional biological hazards in empty cargo containers or impending weather hazards into actionable intelligence. Both of these issues can constitute potential threats to a port and its operation.

In commenting on a draft of this report, Transportation Security Administration officials agreed that the coordination and dissemination of threat information at the port level is an issue that needs to be addressed. They noted that the Transportation Security Administration is overseeing studies (as part of "Operation Safe Commerce") aimed at identifying potential threats and risk mitigation techniques that will contribute to meeting this goal.

Finally, as we have previously reported, DOD uses threat working groups at its installations as a forum to involve installation force protection personnel with local, state, and federal law enforcement officials to identify potential threats to the installation and to improve communication between these organizations.[8] These working groups help coordinate as much information as possible on a broad range of potential threats. Given the limited information available on threats posed by terrorist groups or individuals, such a mechanism assists the installation commander and local authorities in gaining a more complete picture of internal and

[7] Asymmetric threats include unconventional approaches (such as terrorism, the use or threatened use of weapons of mass destruction, and information warfare) that circumvent traditional U.S. military strengths.

[8] U.S. General Accounting Office, *Combating Terrorism: Actions Needed to Improve Antiterrorism Program Implementation and Management*, GAO-01-909 (Washington, D.C.: Sept. 19, 2001).

external threats on a more continuous basis over and above what is provided by an annual threat assessment.

Recent Efforts and Proposed Legislation May Assist Port Security Improvements

Since the September 11 attacks, the Coast Guard and other agencies at ports have made efforts to improve risk management and security measures. The Coast Guard, traditionally a multimission organization, has made a significant shift in operational focus toward seaport security. In so doing, the Coast Guard, in the months immediately following September 2001, diverted resources from other missions such as drug interdiction but has since restored some of its effort in those areas.

Examples of additional recent efforts by the Coast Guard and other agencies include

- formation of Coast Guard maritime safety and security teams based at selected ports to assist in providing port security personnel and equipment;
- Coast Guard escorts or boarding of high-risk ships, including cruise ships, in ports;
- Coast Guard escorts for naval vessels;
- establishment and enforcement of new security zones and increased harbor security patrols (figure 3); and
- port authority cost estimates for improving facility security and interim security improvement measures.

In commenting on a draft of this report, Transportation Security Administration officials indicated that they are taking initial steps toward accomplishing seaport security goals by awarding approximately $217 million in grants (funded through both regular and emergency appropriations) to public and private entities at the ports for initial security assessments, preliminary security improvements, and port incident response training.

Figure 3: Coast Guard Crew in a Rigid Hull Inflatable Boat Demonstrating Enforcement of a Security Zone at a Commercial Port

Source: GAO.

Legislation on maritime security before the Congress (as of October 22, 2002)[9] may promote and enhance these seaport security efforts. Some of the major provisions include

- vulnerability assessments to be conducted at ports;
- establishment of port security committees at each port, with broad representation by relevant agencies, to plan and oversee security measures;
- development of standardized port security plans;
- background checks and access control to sensitive areas for port workers; and
- federal grants for security improvements.

[9] S. 1214 passed the Senate on December 20, 2001. The House of Representatives passed an amendment to S. 1214 on June 4, 2002.

On the basis of our discussions with agency officials at the ports we visited, we believe that if enacted and properly implemented, these and other provisions of the maritime security legislation should assist officials in addressing many of the weaknesses we have identified. For example, comprehensive vulnerability assessments and the proposed standardized security plans could provide a more consistent approach to identifying and mitigating security weaknesses. In providing for port security committees and interagency coordination, the legislation would also provide a framework for organizations at seaports to establish a mechanism to coordinate, analyze, and disseminate threat information at the port level. There may be challenges, however, to implementing the maritime security legislation, including uncertainty about the amount and sources of funds needed to address security needs at seaports. We recently reported on these and other challenges to implementing the provisions of this legislation and the establishment of a new Department of Homeland Security.[10]

In commenting on a draft of this report, Coast Guard officials reported that notwithstanding the status of the proposed legislation, port security committees have already been established at some major ports and that the Coast Guard is preparing a nationwide policy to delineate the purpose and composition of these committees. Coast Guard officials believe that in addition to consideration of vulnerabilities and security planning, the port security committees, as currently envisioned, may provide a more effective mechanism for threat information coordination.

Weaknesses in DOD Force Protection Process Increase Risks for Deployments through Domestic Seaports

During our review, we identified two significant weaknesses in DOD's force protection process. First, DOD lacks a central authority responsible for overseeing force protection measures of DOD organizations while carrying out the various domestic phases of military deployments to and through U.S. seaports. As a result, potential force protection gaps and weaknesses requiring attention and action might be overlooked. Second, there are instances during some phases of these deployments when DOD transfers custody of its military equipment to nongovernment entities. At these times, the equipment could fall into the hands of individuals or groups whose interests are counter to those of the United States.

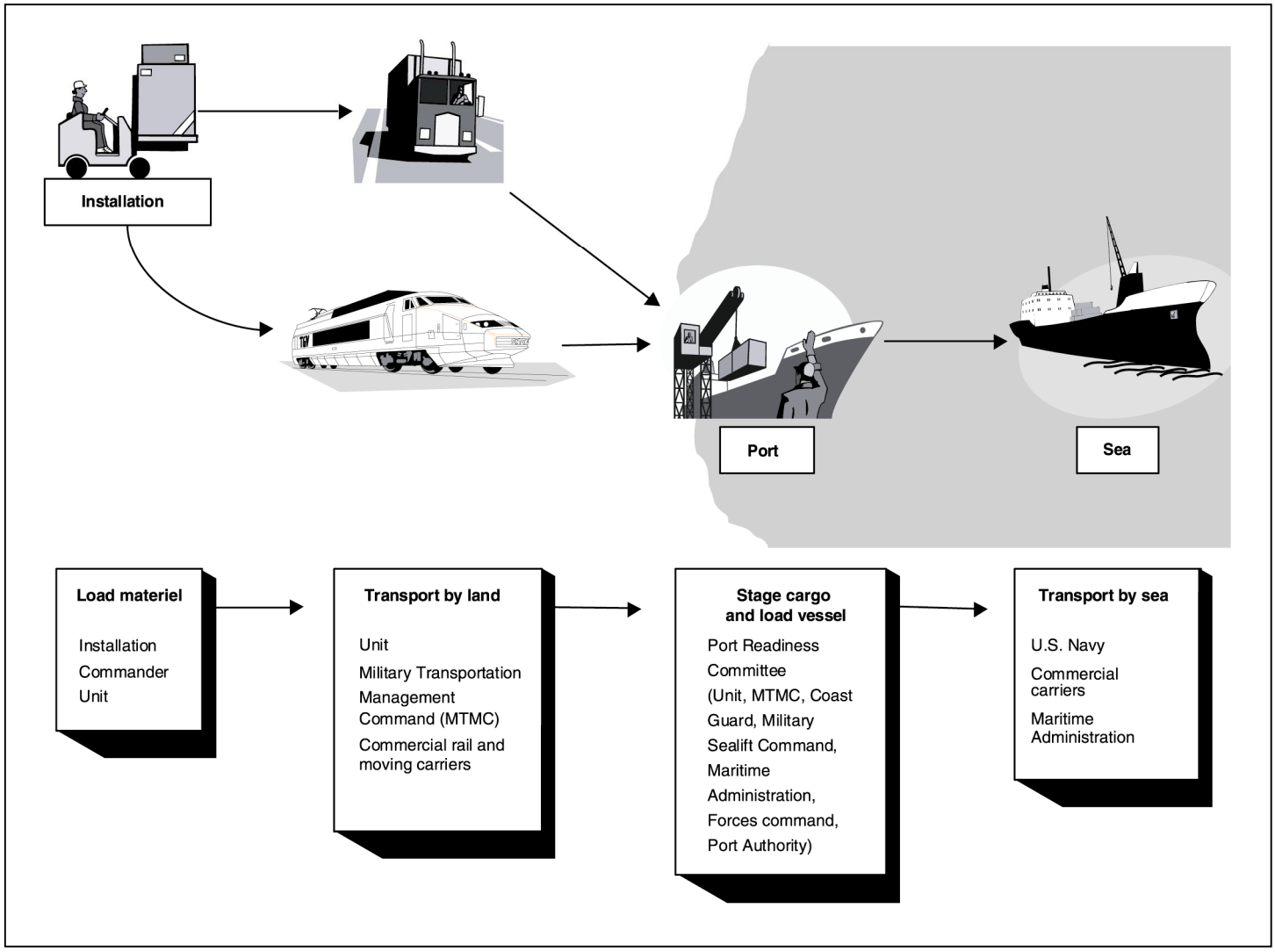
[10] U.S. General Accounting Office, *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful*, GAO-02-993T (Washington, D.C.: Aug. 5, 2002).

DOD Lacks a Central Authority to Coordinate and Execute Domestic Force Protection Measures

Deploying units traditionally focus their force protection efforts primarily on their overseas operations. Before they arrive in an overseas region, the units are required to submit force protection plans to the unified combatant commanders, who are responsible for force protection of all military units in their regions, with the exception of DOD personnel assigned to the Department of State. The tactics, techniques, and procedures in the units' plans must match the guidance developed by the unified commander, who coordinates and approves the individual plans. This allows the commander to ensure that a unit's plan takes into account all current threats that could affect the mission and to accept or mitigate any security risks that arise.

The situation for the domestic phases of overseas deployments is different: there is no designated commander with centralized force protection responsibilities similar to those of the overseas unified combatant commander. This creates gaps, during the domestic phases of a deployment, in DOD's ability to coordinate individual force protection plans, identify gaps that may exist, and mitigate the identified risk. The one coordination mechanism that is in place—the Port Readiness Committee—is focused largely on port operations and at this time does not coordinate all phases of a deployment from an installation through the port. Figure 4 illustrates the domestic phases of a deployment and key organizations responsible for force protection.

Figure 4: The Domestic Phases of the Deployment Process and Responsible Organizations



Source: GAO, based on DOD information.

In the deployments we reviewed, service guidance and DOD antiterrorism standards, particularly those that emphasize the elements of risk management (such as Army major command force protection operations orders), were not always followed in all phases of a deployment from an installation through a port. For example, the Military Traffic Management Command's transportation units recognized the vulnerability of seaport operations and prepared security plans for deployment operations at the ports that were based on assessments of threats, vulnerabilities, and

critical infrastructure. The transport of military equipment to the port by commercial carrier was not always supported by such detailed plans and assessments. In contrast, we found that when a military unit travels by road to a seaport in its own convoy, it generally follows exhaustive planning and risk management measures.

In discussing the absence of a focal point for coordinating and executing force protection measures for the domestic phases of military deployments, DOD officials indicated that the recently established U.S. Northern Command may serve as such a coordinating mechanism. Additionally, in commenting on a draft of this report, DOD officials noted that the principal defense guidance on military transportation issues[11] is in the process of being revised to incorporate force protection guidance.

Military Equipment and Cargo Are Sometimes Not under DOD Control

During deployments from domestic installations through commercial seaports, there are three phases in which DOD either transfers custody of its equipment to nongovernment persons (in some cases foreign nationals) or does not have adequate information about who is handling its equipment, as follows:

- Private trucking and railroad carriers transport equipment and cargo from military installations to seaports.
- Civilian port workers handle and load equipment onto ships.
- Private shipping companies with civilian crews sometimes transport DOD equipment overseas.

The four deployments we reviewed from three military installations in 2001 involved the use of road and rail contract carriers transporting equipment from the installation to a port of embarkation. Contract carriers are required to provide security for the equipment they transport, including sensitive items. For example, contract carriers are required to provide their own security at railroad switching yards, rest areas, overnight stops, and along the entire route whenever they transport sensitive equipment. Although we did not review the steps taken by DOD to evaluate the contractors' security measures, the transfer of accountability to these nongovernmental agents creates a gap in DOD's oversight of its assets between installations and ports.

[11] DOD Directive 4500.9, *Transportation and Traffic Management*, Jan. 26, 1989.

Once equipment arrives at a commercial seaport, it comes under the control of the military units responsible for managing the loading process. However, civilian port workers, stevedores, and longshoremen—who undergo limited screening and background checks by port authorities or terminal operators—handle military equipment and cargo, as well as the loading and unloading of ships used to transport the equipment overseas. This was the case in all the deployments we reviewed. In all cases, the stevedores or longshoremen were in the same labor pool as the one used for commercial port operations. While DOD officials have not identified port workers as a particular threat, they are concerned that lack of information on the background of individuals handling military equipment increases potential risk. Organizations at some of the ports we visited are now implementing or reviewing efforts to increase screening of port workers. And the maritime security legislation currently before the Congress includes provisions for background checks and access control for port workers. These measures, if approved and properly implemented, may help address this issue. In commenting on a draft of this report, Transportation Security Administration officials acknowledged the problems posed by the lack of screening for port workers and indicated that they plan to study and eventually issue nationwide standards for credentialing port workers.

DOD also transfers custody of its equipment when the equipment is placed aboard a commercial ship for transport overseas. We reviewed four major overseas deployments from three military installations during calendar year 2001 that involved about 6,550 tons of military equipment and supplies. Although these four deployments are not representative of all DOD deployments conducted in 2001, they do illustrate the use of foreign-owned commercial vessels by DOD. In commenting on a draft of this report, DOD officials stated that about 43 percent of cargo shipped overseas in 2001 as part of deployments involving major equipment in support of overseas operations was carried on foreign-flagged ships.[12] As indicated in table 1, most of the ships for the deployments we reviewed were both foreign-owned and foreign-crewed.

[12] DOD further stated that only 18 percent of all cargo (including deployments and general cargo, such as household goods) shipped by the Military Sealift Command was transported by foreign-flagged vessels.

Table 1: Ownership and Crew for Commercial Ships Used in Deployments GAO Reviewed from Three Installations in 2001

Ship	U.S. Owned	Foreign Owned	U.S. Crew	Foreign Crew
1	●		●	
2	●			●
3		●		●
4		●		●
5		●		●
6		●		●
7		●		●
8		●	N/A	N/A
9		●	N/A	N/A

N/A: Crew information not available.

Source: DOD.

In addition to transferring custody over its assets to non-DOD personnel, DOD did not generally provide security forces aboard these vessels. Several of the ships used in the deployments we reviewed did have DOD maintenance personnel aboard, but the ship manifests did not indicate that armed DOD personnel were aboard as a security force. The Military Sealift Command reviews charter vessel crew lists to determine whether any crewmembers are known security threats. Some of the materiel transported by these vessels included sensitive and mission essential items. Table 2 provides examples of equipment carried aboard foreign-owned and foreign-crewed ships for the deployments we reviewed.

Table 2: Examples of Equipment Carried on Foreign-Owned and Foreign-Crewed Ships

Equipment Category	Example
Major weapon system	• Bradley fighting vehicles • 155mm howitzers • Apache attack helicopters • Blackhawk helicopters • Stinger anti-aircraft launchers • Armored light vehicles
Other weapons	• Antitank missile launchers • .50 caliber machineguns • 40mm grenade launchers • 9mm pistols • M-16A2 rifles • Squad automatic weapons • Bayonets

Equipment Category	Example
Individual equipment	• Night vision goggles • Minefield marking system • Chemical agent monitor • Body armor • Nuclear, biological, and chemical protective suits and masks • Mine detection sets • Global positioning system receivers
Communications equipment	• Radio sets • Antenna assemblies • Satellite communications terminals

Source: DOD.

When DOD relinquishes control over its equipment, it relies on nongovernment third parties to protect its assets. Placing military equipment outside DOD's control also complicates the steps needed to mitigate the higher risk and could disrupt military units from performing their intended missions. An example of the dangers of such loss of control occurred in summer 2000. While in the North Atlantic, the captain of a commercial vessel carrying Canadian military equipment and three Canadian Forces personnel from the Balkans refused to proceed to the ship's destination port in Canada after a dispute over payment to the vessel's owner. The vessel, GTS *Katie*, was owned by a U.S. company but registered in St. Vincent and the Grenadines and crewed by non-U.S. citizens. Alarmed at the loss of control over its equipment, including sensitive items, the Canadian government was compelled to board the *Katie* with a contingent of Canadian Forces naval personnel from a nearby warship. The vessel was then brought safely into a Canadian port.[13]

The Canadian Defense Minister explained that the loss of control over military equipment compromised Canada's ongoing military operations and the ability to undertake new ones.[14] Similarly, when the third parties to whom DOD relinquishes control of its equipment include foreign nationals, there may be an increased risk of the equipment being tampered with, seized, or destroyed by individuals or groups whose interests run

[13] The Department of Defense had also chartered the same vessel to transport military equipment from operations in the Balkans.

[14] Although he recognized the danger of the *Katie* incident, the Canadian Defense Minister also acknowledged that it would still be necessary for Canada to charter nongovernment vessels for future military movements.

counter to those of the United States and an increased chance that those weapons or equipment might be used against military or civilian targets.

During our review, officials from several military commands expressed concern about placing military equipment aboard ships that are outside DOD control. DOD officials told us that the reasons for the use of commercial contract carriers include, among others, economy and efficiency over using government-owned and -operated vessels and the adequacy and availability of the U.S.-flagged merchant marine. In commenting on a draft of this report, Maritime Administration officials agreed with our concerns related to the use of foreign ships and crews to transport sensitive military equipment and reiterated their interest in increasing the number of U.S.-flag vessels appropriate for DOD use. They indicated that the shortage of appropriate U.S.-flagged ships will be exacerbated by Military Sealift Command plans to terminate existing charters for some U.S.-flag vessels.

Conclusions

The events of September 11 highlighted the vulnerability of the U.S. homeland to unconventional attack, and the resulting new security environment warrants that more attention be paid to the domestic phases of military deployments. It is clearly evident that since September 11, DOD and the organizations responsible for seaport security recognize the need for increased vigilance at home during the domestic phases of a military deployment, and this recognition provides an opportunity to improve seaport security in a systematic and effective manner.

However, the inadequate assessment of threats and vulnerabilities and lack of comprehensive security plans prevent organizations at seaports and DOD from thoroughly analyzing the security environment at the ports. This hampers the identification and prioritization of requirements for the protection of critical assets. This situation compounds an already difficult task of protecting deploying DOD forces. However, if enacted and properly implemented, pending maritime security legislation would address most of these issues. We are therefore making no recommendations in this area.

The absence of a mechanism at the strategic seaports for coordinating and disseminating comprehensive threat information increases the risk that threats—both traditional and nontraditional—will not be identified and appropriately communicated to all relevant organizations. If established at the port level such a mechanism could provide a formal, rather than informal and ad-hoc, process for coordinating information, and it could

focus on port-specific threats, rather than a regionwide perspective. A central coordination mechanism could also provide a means to analyze threats on a continuous basis.

Without a DOD authority or organization to coordinate force protection planning and execution for the domestic phases of DOD deployments to and through strategic seaports, potential gaps in force protection may go unnoticed, increasing the risk to DOD operations and equipment. Having such an authority would not only reduce such risks, but would also provide oversight to ensure that risk management and antiterrorism standards are consistently applied through all phases of a deployment from an installation through a port.

When military equipment is entrusted to non-DOD personnel, with limited DOD control over the equipment, there is a greater risk that it could be tampered with, seized, or destroyed. While we recognize there are times during a deployment when DOD will relinquish direct control of its equipment, the new security environment warrants that DOD re-evaluate its current policies and procedures to ensure that appropriate security measures are applied during these times. Weaknesses in DOD's force protection approach along with uncertainties in the security environment at strategic seaports result in increased risks that military operations could be disrupted, successful terrorist attacks might occur, or sophisticated military equipment might be seized by individuals or organizations whose interests run counter to those of the United States.

Recommendations for Executive Action

To improve the information available to develop effective seaport security measures, we recommend that the Secretary of Transportation identify and direct the appropriate transportation agency to develop a mechanism at the port level to compile, coordinate, analyze, and disseminate threat information on a real-time basis to all relevant organizations. Such a mechanism might be similar to DOD's threat working groups but with broader membership or be part of an existing coordinating body (such as the proposed port security committees or the joint terrorism task forces). Whether established as a new entity or as a modification of an existing coordinating body, this mechanism should include representatives from a broad range of federal, state, and local agencies. It should also include in its assessment process nontraditional threats such as natural emergencies and information technology attacks.

To improve DOD's oversight and execution of force protection for deployments to and through domestic strategic seaports, we recommend that the Secretary of Defense

- designate a single authority (such as the recently established U.S. Northern Command) to coordinate and execute force protection planning for deployments of units from installations in the United States through seaports and until ships enter the destination areas of operation (this responsibility would be similar to that of the overseas unified combatant commands for their respective areas of operation) and
- direct the single coordinating authority (once established), along with the U.S. Transportation Command, to develop and implement measures to maintain greater security over equipment transported by non-DOD carriers.

Agency Comments and Our Review

DOD agreed with the need for a single DOD authority to coordinate and execute force protection planning for deployments from installations in the United States through seaports and until ships enter the destination areas of operation. In commenting on this report, DOD stated that the recently established U.S. Northern Command will work closely with the U.S. Transportation Command to examine security for deployments through domestic seaports.

DOD also agreed with the need for measures to maintain greater security over equipment transported by non-DOD carriers. In its comments, however, DOD stated that it has for decades relied on the commercial sector to provide a large portion of the nation's strategic sealift capabilities in both peacetime and during contingencies and that it is not cost effective to use government-owned sealift vessels for routine cargo movements or force rotations of the type included in GAO's analysis. Nonetheless, DOD stated that the U.S. Transportation Command and the new U.S. Northern Command will continue to seek ways to improve the security of DOD cargo transported via commercial carrier, including the use of satellite tracking of cargo and vessels and placing security personnel aboard those ships. On those occasions when DOD transfers custody of its equipment to non-DOD carriers, the kinds of additional measures DOD discussed should help improve the overall security of sensitive DOD cargoes.

DOD's written comments are included in their entirety in appendix II. In addition, DOD officials suggested a number of technical clarifications and

corrections, which we have incorporated into this report where appropriate.

In oral comments on a draft of this report, Department of Transportation officials generally agreed with the findings, conclusions, and recommendations. They also provided additional information and suggested a number of technical clarifications and corrections, which we have incorporated into this report where appropriate. Transportation officials discussed several new and ongoing efforts affecting seaport security by the newly established Transportation Security Administration. Among other initiatives, these include measures for seaport security grants, studies on credentialing port workers, and a study on developing a threat assessment center. These initiatives are funded through regular and emergency appropriations for fiscal year 2002. Additionally, proposed appropriations for fiscal year 2003 would provide further funding if enacted into law. If properly implemented, these initiatives should contribute to the goal of improved seaport security.

As arranged with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from its issue date. At that time, we will send copies to the Secretaries of Defense and Transportation and interested congressional committees. We will also make copies available to others upon request. In addition, the report will be available at no cost on the GAO Web site at http://gao.gov.

If you or your staff have any questions regarding this report, or wish to discuss this matter further, please contact me at (202) 512-6020. Key contributors are acknowledged in appendix III.

Sincerely yours,

Raymond J. Decker, Director
Defense Capabilities and Management

Appendix I: Scope and Methodology

To analyze the security environment at strategic seaports we reviewed security planning and procedures during the conduct of site visits at six selected commercial seaports and two military-owned ammunition ports. These six commercial ports included ports that regularly support DOD deployments as well as those that are used less frequently. We selected ports on the West Coast, East Coast and on the Gulf of Mexico. We visited two of the three dedicated ammunition ports identified by DOD, one on each coast. For security reasons, we do not discuss location-specific information in this report.

At these selected ports we reviewed documents, observed security measures, and discussed port operations, security planning, coordination mechanisms, specific vulnerabilities, mitigation plans, and resource issues with government and nongovernment officials. Among the organizations we visited during our seaport visits were the Coast Guard, the U.S. Maritime Administration, the Federal Bureau of Investigation, the U.S. Customs Service, port authorities, and local law enforcement agencies. Although the information we obtained at these locations could not be generalized to describe the environment DOD could expect at all seaports, it provides insight into what DOD could expect to encounter at domestic seaports. We also discussed these issues with officials at Coast Guard headquarters and the U.S. Maritime Administration, both in the Department of Transportation in Washington, D.C.

To analyze DOD's process for securing deployments of military equipment through strategic seaports we examined force protection plans, procedures, and coordination measures for four deployments conducted in 2001. We selected these deployments based on information provided by the U.S. Army Forces Command. The command provided a list of deployments involving units moving from within the continental United States to an overseas location during calendar year 2001 that required the use of sealift to transport military equipment. We selected four deployments originating from three installations in calendar year 2001 because they represented about 65 percent of the total tonnage of equipment for all deployments to major DOD contingency operations during that period. An additional factor in our selection was the geographic dispersion of the domestic seaports used for the deployments.

Our review of force protection procedures included the guidance and criteria for force protection for deployments, the extent to which these are clearly defined and carried out, and the extent to which DOD works with other federal, state, and local agencies to plan and carry out force protection measures. We also reviewed information from the Military

Sealift Command and Military Traffic Management Command on the ships used to transport equipment for these deployments and the equipment they carried. We interviewed officials from the following organizations:

- Office of Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict in Washington, D.C.
- U.S. Transportation Command at Scott Air Force Base, Ill.
  - Military Transportation Management Command in Fort Eustis, Va.
  - Military Sealift Command in Washington, D.C.
- U.S. Central Command in Tampa, Fla.
- U.S. Army Forces Command in Atlanta, Ga.
- Army and Navy Force Protection Offices in Washington D.C.
- Transportation and force protection officials at the installation and unit levels for Army and Marine Corps units

To examine DOD force protection efforts, we conducted site visits at three military installations that were the origins of the four 2001 deployments in our review. During these site visits, we reviewed DOD force protection plans, policies and standards used for the equipment involved in the deployments and discussed with unit and installation personnel how DOD addressed security weaknesses identified at the seaports. We also discussed the experience of past deployments and recent deployments with DOD officials at installations and the ports.

We also reviewed the findings and recommendations of the Interagency Commission of Crime and Security in U.S. Seaports and the provisions of maritime security legislation now before Congress to determine the potential impact on current and future seaport security efforts. We analyzed the provisions of both House and Senate versions of the legislation and discussed key provisions with staff members of cognizant Congressional committees.

We conducted our review from January through August 2002 in accordance with generally accepted government auditing standards.

Appendix II: Comments from the Department of Defense

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301-2500

SPECIAL OPERATIONS/
LOW-INTENSITY CONFLICT

OCT 4 2002

Mr. Raymond J. Decker
Director, Defense Capabilities Management
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Decker:

The Department of Defense (DoD) has reviewed the GAO draft report, GAO-03-15, "COMBATING TERRORISM: Actions Needed to Improve Force Protection for DoD Deployments Through Domestic Seaports," dated October 2002 (GAO Code 350156). The draft report reflects an extensive research and reporting effort by your analysis team.

The Department concurs with comment on the two recommendations (Tab A) in the report. Additionally, technical comments have been forwarded to your staff to correct and clarify information in selected sections of the report.

Sincerely,

Marshall Billingslea
Principal Deputy

Enclosures:
As stated

Prepared by: CDR Carlos E. Aponte, (703) 697-3254

GAO DRAFT REPORT – DATED OCTOBER 2002
GAO-03-15 / CODE 350156

"COMBATING TERRORISM: Actions Needed to Improve Force Protection for DoD Deployments Through Domestic Seaports"

DEPARTMENT OF DEFENSE RESPONSE TO THE RECOMMENDATIONS

RECOMMENDATION 1: To improve DoD's oversight of force protection for deployments to and through domestic strategic seaports, we recommend that the Secretary of Defense designate a single authority (such as the recently proposed U.S. Northern Command) to coordinate and execute force protection planning for deployments of units from installations in the United States through seaports and until ships enter the destination areas of operation (this responsibility would be similar to that of the overseas unified combatant commands for their respective areas of operation).
(pp. 23-24/GAO Draft Report)

DoD RESPONSE: Concur. USNORTHCOM was recently established as a combatant command with regional responsibility for the express purpose of coordinating DoD's Homeland Security efforts within CONUS. USTRANSCOM will work closely with USNORTHCOM in the coming months to examine security for deployments through domestic seaports.

RECOMMENDATION 2: To improve DoD's oversight of force protection for deployments to and through domestic strategic seaports, we recommend that the Secretary of Defense direct the single coordination authority (once established), along with the U.S. Transportation Command, to develop and implement measures to maintain greater security over equipment transported by non-DoD carriers.
(p. 24/GAO Draft Report)

DoD RESPONSE: Partially concur. It must be understood that DoD has, for decades, relied upon the commercial sector to provide a large portion of the nation's strategic sealift capability in both peacetime and during contingency. This reliance is borne both out of necessity and for cost reasons. Military Sealift Command maintains a fleet of government owned strategic sealift vessels that are intended to surge into action in event of a large-scale deployment. In such a contingency, these vessels will be used primarily to move our most critical war fighting equipment and supplies, such as deploying war fighting forces and munitions. However, it is not cost effective to use this fleet for routine cargo movement or deployment of forces for exercises or force rotations. Military Sealift Command does decide what type of vessel should be used (be it U.S. government owned or leased, U.S. flagged commercial or foreign flagged commercial) based, in part, on the type of cargo to be shipped and the perceived threat to that cargo and vessel.

The necessity for using non-DoD carriers will continue for both routine movements of cargo absent a contingency as well as to support an increased flow of cargo in the event of one. USTRANSCOM will work with USNORTHCOM and the Services to continue to improve the security of DoD cargo moved via commercial carriers. Satellites tracking cargo and vessels, as well as increased use of Supercargos (security personnel aboard vessels), are two methods that we are moving forward with.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Ray Decker (202) 512-6020

Bob Repasky (202) 512-9868

Staff Acknowledgements

In addition to those names above, Willie J. Cheely, Jr., Brian G. Hackett, Joseph W. Kirschbaum, Jean M. Orland, Stefano Petrucci, Elizabeth G. Ryan, and Tracy M. Whitaker also made key contributions to this report.

Related GAO Products

Homeland Security: Department of Justice's Response to Its Congressional Mandate to Assess and Report on Chemical Industry Vulnerabilities. GAO-03-24R. Washington, D.C.: October 10, 2002.

Homeland Security: Information Sharing Activities Face Continued Management Challenges. GAO-02-1122T. Washington, D.C.: October 1, 2002.

Combating Terrorism: Department of State Programs to Combat Terrorism Abroad. GAO-02-1021. Washington, D.C.: September 6, 2002.

National Preparedness: Technology and Information Sharing Challenges. GAO-02-1048R. Washington, D.C.: August 30, 2002.

Homeland Security: Effective Intergovernmental Coordination is Key to Success. GAO-02-1013T. Washington, D.C.: August 23, 2002.

Homeland Security: Effective Intergovernmental Coordination is Key to Success. GAO-02-1012T. Washington, D.C.: August 22, 2002.

Homeland Security: Effective Intergovernmental Coordination Is Key to Success. GAO-02-1011T. Washington, D.C.: August 20, 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.

Homeland Security: Critical Design and Implementation Issues. GAO-02-957T. Washington, D.C.: July 17, 2002.

Homeland Security: Title III of the Homeland Security Act of 2002. GAO-02-927T. Washington, D.C.: July 9, 2002.

Homeland Security: Intergovernmental Coordination and Partnerships Will Be Critical to Success. GAO-02-899T. Washington, D.C.: July 1, 2002.

Homeland Security: New Department Could Improve Coordination but May Complicate Priority Setting. GAO-02-893T. Washington, D.C.: June 28, 2002.

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

Homeland Security: Key Elements to Unify Efforts Are Underway but Uncertainty Remains. GAO-02-610. Washington, D.C.: June 7, 2002.

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

Homeland Security: Responsibility And Accountability For Achieving National Goals. GAO-02-627T. Washington, D.C.: April 11, 2002.

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

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

Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy. GAO-02-549T. Washington, D.C.: March 28, 2002.

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

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

Homeland Security: Progress Made; More Direction and Partnership Sought. GAO-02-490T. Washington, D.C.: March 12, 2002.

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

Homeland Security: Challenges and Strategies in Addressing Short- and Long-Term National Needs. GAO-02-160T. Washington, D.C.: November 7, 2001.

Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts. GAO-02-208T. Washington, D.C.: October 31, 2001.

Combating Terrorism: Considerations For Investing Resources in Chemical and Biological Preparedness. GAO-01-162T. Washington, D.C.: October 17, 2001.

Homeland Security: Key Elements of a Risk Management Approach. GAO-02-150T. Washington, D.C.: October 12, 2001.

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

Combating Terrorism: Selected Challenges and Related Recommendations. GAO-01-822. Washington, D.C.: September 20, 2001.

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

GAO's Mission

The General Accounting Office, the 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

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. General Accounting 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

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548