United States General Accounting Office

GAO

Report to the Chairman, Special Oversight Panel on Terrorism, Committee on Armed Services, House of Representatives

November 2002

COMBATING TERRORISM

Actions Needed to Guide Services' Antiterrorism Efforts at Installations

GAO-03-14

Contents

Abbreviations

DOD	Department of Defense
GAO	General Accounting Office

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

November 1, 2002

The Honorable Jim Saxton
Chairman, Special Oversight Panel on Terrorism
Committee on Armed Services
House of Representatives

Dear Mr. Chairman:

After the September 11, 2001, terrorist attacks, domestic military installations increased their antiterrorism measures[1] to their highest levels. These measures were reduced in the weeks following the World Trade Center and Pentagon attacks, but because of the persistent nature of the threat, the antiterrorism posture at domestic installations remains at a higher than normal level more than 1 year later. The Department of Defense's (DOD) budget request for fiscal year 2003 includes over $10 billion for combating terrorism activities,[2] which includes a substantial increase in funding for antiterrorism measures to safeguard personnel and strategic assets.

We previously examined the implementation of DOD's antiterrorism initiatives, and focused on the measures taken by domestic military installations to reduce vulnerabilities last year. We reported that at the departmental level, the antiterrorism efforts lacked critical management elements, such as a strategic plan containing long-term goals and a performance plan to measure results, assess progress, and identify corrective actions.[3] To strengthen the management of the antiterrorism

[1] Antiterrorism represents defensive measures used to reduce the vulnerability of individuals and property to terrorist acts. Examples of defensive measures include reducing the number of access points onto an installation, verifying the identity of personnel entering installations, increasing security patrol activity at high-risk targets, and issuing weapons to all security and law enforcement personnel.

[2] Antiterrorism constitutes only one of four combating terrorism categories. The other three categories are counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), consequence management (preparation for and response to a terrorist attack), and intelligence support (collection, analysis, and dissemination of terrorism-related information).

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

program, we recommended that DOD establish a management framework containing these elements, which could then provide a vehicle to guide resource allocations and measure the results of DOD's improvement efforts. DOD agreed with this recommendation and initiated steps to develop the framework but temporarily suspended these efforts after the terrorist attacks on September 11, 2001. The Department has recently restarted these efforts.

If consistent with our previous recommendation, this forthcoming Department-wide framework should represent a significant and important shift in management focus—from measuring program activities and processes to measuring program results. To supplement and support this results-oriented approach, a comprehensive risk management process can be an effective foundation for allocating antiterrorism resources. Risk management is a systematic, analytical process to determine the likelihood that a threat will harm individuals or physical assets and to identify actions to reduce risk and mitigate the consequences of a terrorist attack. (More detailed information on risk management appears in the background section of this report.)

Because of the increased emphasis on and funding for DOD's antiterrorism efforts, you asked us to examine the management framework each military Department has established to implement antiterrorism initiatives. Accordingly, this report specifically focuses on the extent to which the military services and selected commands (1) use a results-oriented management framework to guide their antiterrorism efforts at domestic installations[4] and (2) have established an effective risk management approach to develop specific antiterrorism requirements. Because you also asked us to examine how DOD reports combating terrorism funding, we also reviewed funding trends and determined whether DOD's annual budget reports to Congress completely and accurately portray funding for combating terrorism.

To accomplish this work, we obtained and reviewed documents, examined the operations of the four services' headquarters, examined the operations of eight major service commands and reserve components, and interviewed cognizant officials. Collectively, these eight commands have

[4] "Domestic" refers to the continental United States and excludes Alaska, Hawaii, and the U.S. territories.

antiterrorism responsibilities for approximately 444 installations.[5] Although the information we obtained at these commands cannot be generalized to describe the Department's overall antiterrorism efforts, it provides insights into the antiterrorism programs within these commands. Further information on our scope and methodology appears in appendix I.

Results in Brief

For the most part, the service headquarters and commands we reviewed did not use a comprehensive results-oriented management framework to guide their antiterrorism efforts. For example, resource decisions generally were not made with reference to specific, long-term goals, and short-term measurable performance goals had not been set. However, 3 of the 12 organizations included in our review—Air Force headquarters, Army Forces Command, and the Navy's Atlantic Fleet—did have some, but not all, elements of a results-oriented management framework in place. The Army Forces Command's management framework appeared to be the most complete, containing elements such as long-term and annual goals, clear performance measures, quarterly reviews, and the identification of resource requirements. The Forces Command's framework also appeared to have strong support from senior command officials, without which it might not have been as fully implemented. According to service officials, a comprehensive results-oriented management framework for antiterrorism efforts is not consistently used across all services and commands because DOD does not require it, and service officials indicated that they were reluctant to develop such an approach before the forthcoming DOD-wide antiterrorism strategy was issued. Although the Department has recently restarted its efforts toward developing this strategy, it has not set a specific time frame for its completion. Without a results-oriented management framework at both DOD and the service levels to prioritize, integrate, and evaluate antiterrorism initiatives, the services and commands may not be efficiently allocating the significant resources currently applied to antiterrorism efforts or effectively assessing progress in safeguarding military personnel and assets.

The services and commands we reviewed are generally following prescribed guidance and regulations to conduct risk management analyses (i.e., terrorist threat, vulnerability, and asset criticality assessments) to support their antiterrorism requirements, but significant weaknesses exist

[5] The number of installations is based on information provided by the respective commands.

with the current approach. Each service has established requirements for installations to use a risk management approach in developing funding requirements and generally provided implementing guidance on preparing the assessments; in addition, each command verified that assessments have been completed. However, weaknesses exist in the services' oversight of this process. Specifically, the commands do not always require documentation of the assessments, and they do not periodically evaluate the assessment methodology used at each installation to determine the thoroughness of the analyses or the consistency with required assessment methodology. If the services and commands do not evaluate installation assessments and do not require the documentation of all assessments, then they have no assurance that installations' antiterrorism requirements are based on a rigorous application of risk management principles or that these assessments produce comparable results across a service. Consequently, when the services consolidate their antiterrorism requirements, the result may not accurately reflect the most pressing needs.

DOD has reported that $32.1 billion has been allocated or requested for combating terrorism activities from fiscal year 1999 through fiscal year 2003; however, these reported amounts may not present a clear picture of total combating terrorism costs. Our analysis indicates that $19.4 billion (60 percent) of this amount is for military and civilian personnel and personnel-related operating costs associated with individuals in designated specialties that have combating terrorism-related missions, such as military police, civilian police, and security guards. This allocation may overstate actual combating terrorism costs, however, because the military services accounting systems do not track the actual time that these individuals spend on activities related to combating terrorism. Consequently, the total funding allocated to these personnel specialties are included in the report, even if the individuals spend only a portion of their time performing combating terrorism activities.

We are recommending that DOD accelerate its efforts to develop a Department-wide strategy, set a target date for its completion, and work with the military services to concurrently initiate steps to adopt a results-based management framework for their antiterrorism efforts that is consistent with this Department-wide approach. We also are recommending that the services take steps to improve their risk management approaches that underpin antiterrorism requirements. Additionally, we are recommending that steps be taken to clarify DOD's combating terrorism budget report provided to Congress. In written comments on a draft of this report, DOD agreed with all of our

recommendations and it identified actions that are under way at the Department to address these recommendations.

Background

DOD's Antiterrorism Policy and Guidance

DOD issued a directive[6] signed by the Deputy Secretary of Defense that provides DOD's antiterrorism policy and assigns responsibilities to DOD organizations for implementing antiterrorism initiatives. This directive places responsibility for developing antiterrorism policy and guidance with the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict.[7] In this capacity, the Assistant Secretary of Defense issued an instruction that established 31 antiterrorism standards that DOD organizations, including the services, are required to implement.[8, 9] These standards address antiterrorism planning, training requirements, physical security measures, and related issues. The office also issued a handbook containing additional detailed guidance on antiterrorism policies and practices, including guidance on assessment methodology.[10] The Joint Staff has also issued an installation-planning template to help installations prepare their antiterrorism plans.[11] Additionally, each of the services has issued regulations, orders and instructions to implement the DOD guidance and establish its own specific policies and standards. DOD and the services have recently revised some of these key guidance documents, and others are now under revision.

[6] DOD Directive 2000.12, DOD Antiterrorism/Force Protection Program, Apr. 13, 1999.

[7] The Assistant Secretary of Defense for Special Operations and Low Intensity Conflict performs these duties under the Under Secretary of Defense for Policy.

[8] DOD Instruction 2000.16, DOD Antiterrorism Standards, June 14, 2001.

[9] The 31 antiterrorism standards in DOD Instruction 2000.16 also apply to the Office of the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, defense agencies, and field activities.

[10] DOD Handbook O-2000.12-H, Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence, Feb. 19, 1993.

[11] Joint Staff Antiterrorism Force Protection Installation Planning Template, July 1, 1998.

Process for Developing Services' Antiterrorism Requirements

The services assign responsibility for protecting installations from terrorist attacks to installation commanders, who identify and prioritize antiterrorism requirements. Installation commanders are to compose a prioritized list of antiterrorism requirements from annual assessments of threat, vulnerability, and the criticality of assets, which they submit to their respective major commands. The major commands merge the antiterrorism requirements from all of their installations, prioritize them, and forward their integrated list to the service's headquarters. Similarly, the services merge and prioritize the antiterrorism requirements of their major commands, and the consolidated list is then used as a basis for funding decisions.

DOD's Risk Management Approach

The required assessments of threat, vulnerability, and criticality of assets form the foundation of each installation's antiterrorism plan and support a risk management approach to resource allocation. These three assessments are designed to assess (1) the threats to the installation, (2) the installation's vulnerabilities, and (3) the installation's critical assets.

The threat assessment identifies and evaluates potential threats on the basis of such factors as the threats' capabilities, intentions, and past activities. This assessment represents a systematic approach to identify potential threats before they materialize. However, this assessment might not adequately capture some emerging threats, even in cases where the assessment is frequently updated. The risk management approach therefore uses vulnerability and asset criticality assessments as additional inputs to the risk management decision-making process.

A vulnerability assessment identifies weaknesses that may be exploited by identified threats and suggests options that address those weaknesses. For example, a vulnerability assessment might reveal weaknesses in an installation's access control system, its antiterrorism awareness training, or how mission-critical assets such as fuel storage sites and communications centers are protected. Teams of multidisciplinary experts skilled in such areas as structural engineering, physical security, and installation preparedness conduct these assessments.

A criticality assessment evaluates and prioritizes assets and functions to identify which assets and missions are relatively more important to protect from attack. For example, important communications facilities, utilities, or major weapons systems might be identified as critical to the execution of U.S. military war plans, and therefore receive additional protection.

Criticality assessments provide information in order to prioritize resources while at the same time, reducing the potential application of resources on lower-priority assets.

Services' Antiterrorism Efforts Lack a Results-Oriented Management Framework

The critical elements of a results-oriented management framework are not being used by the services to guide their antiterrorism efforts. In results-based management, program effectiveness is measured in terms of outcomes or impact rather than outputs (i.e., activities and processes). Results-oriented principles and elements, which we have derived from the Government Performance and Results Act,[12] are presented in table 1. Benefits from a results-based management approach depend upon the combined use of all eight of the critical elements that appear in the table. These elements, when combined with effective leadership can provide a management framework to guide major programs and activities.

Table 1: Results-Oriented Management Framework Principles

Principle	Critical elements
Strategic plan—defines the program's overall purpose, mission, and intent.	Long-term goals—typically general in nature that lay out what the agency wants to accomplish in the next 5 years.
	Strategies to be used—general methods the agency plans to use to accomplish long-term goals.
	External factors—factors that may significantly affect the agency's ability to accomplish goals.
Performance plan—describes detailed implementation actions as well as measurements and indicators of performance.	Performance goals—stated in objective measurable form.
	Resources—a description of the resources needed to meet the performance goals.
	Performance indicators—mechanisms to measure outcomes of the program.
	Evaluation plan—means to compare and report on program results vs. performance goals.
	Corrective actions—a list of actions needed to address or revise any unmet goals.

Source: Government Performance and Results Act of 1993.

[12] P.L. 103-62. Congress enacted the Government Performance and Results Act in 1993 to provide for, among other things, the establishment of strategic planning and performance measurement in the federal government.

The critical elements of a results-oriented management framework were largely absent in the antiterrorism efforts of three services' headquarters and at six of the eight commands we examined. Specifically, the services have not published and disseminated unambiguous results-based, strategic and performance goals for their antiterrorism efforts. Some service antiterrorism officials did articulate broadly stated goals—such as protecting personnel and material assets against terrorist attack, and defeating terrorism—but these goals have not been endorsed and disseminated by service headquarters as servicewide goals nor have the services described how these goals will be achieved or how they intend to evaluate results in terms of the goals. The Air Force, however, has taken some steps toward a results-based management framework. For example, it has published long-term goals and established service-level working groups to evaluate the effectiveness of its antiterrorism program and identify the actions needed to address or revise any unmet goals. Although the Air Force has taken these positive steps, Air Force officials acknowledge that the elements may not have been effectively articulated servicewide so that installations can understand the "big picture" and how all elements fit together. In fact, officials we contacted from Air Combat Command and Air National Guard were not aware of the service-level goals or performance-planning elements.

At the command level, a results-oriented management framework was largely absent in the antiterrorism efforts of six of the eight major commands we reviewed. For example, the Air Combat Command did not have overarching antiterrorism goals for its 15 bases, although command officials said that they planned to develop them. Also, the Army National Guard has not issued antiterrorism goals for its 3,900 armories and 211 installations and has no plan to do so.

Two of the commands—the Army's Forces Command and the Navy's Atlantic Fleet—adopted aspects of a results-oriented framework, and officials said that they did so on their own initiative and without direction from their parent service. The Army Forces Command management framework contained most of the critical management elements, such as quarterly reviews, long-term and annual goals, clear performance measures, and identification of resource requirements. Army Forces Command officials said that the results-based management approach enables its senior officers to monitor the command's progress toward its short- and long-term goals and make necessary adjustments to the strategy and resource allocation to accomplish these goals. Forces Command officials attributed their management approach's success, in large part, to the involvement of senior command officials and their endorsement of

this management approach. According to Army headquarters antiterrorism officials, the Forces Command management framework has been an effective approach and may be useful as a model for other major commands.

The Navy's Atlantic Fleet Command also articulated long-term goals and strategies to accomplish its antiterrorism goals. For example, the fleet developed a plan of action to address security deficiencies that were identified through assessments by establishing a database to track deficiencies and identify trends. The fleet also linked resource requirements to accomplish these steps and developed metrics to measure results. According to the Atlantic Fleet officials we spoke with, however, these strategies are not currently being used by the fleet to shape its antiterrorism efforts because they are waiting for the Navy to issue servicewide antiterrorism goals. Atlantic Fleet officials stated they wanted to avoid having separate and different strategic plans for each command.

The services and their major commands cite two primary reasons for not employing a results-based management framework to guide and implement their antiterrorism efforts. First, the services do not want to adopt goals and strategies that might prove inconsistent with DOD's forthcoming, Department-wide antiterrorism strategy. As discussed earlier, the Department was in the process of developing an antiterrorism strategy, but suspended its efforts after the attacks on the World Trade Center and the Pentagon because of the pressing needs of the war on terrorism. DOD officials have indicated that they have reinitiated their efforts to develop a strategy but have not set a target date for their completion. The second reason cited by service officials for not employing a results-oriented management framework was that strategic planning and performance planning called for by the Results Act applies to agencies and not to specific efforts such as antiterrorism. We agree that the services and major commands are not required by the Results Act to prepare strategic plans and performance plans specific to their antiterrorism efforts. Nonetheless, the Results Act offers a model for developing an effective management framework to improve the likelihood of successfully implementing initiatives and assessing results.

Without a results-based management approach to prioritize, integrate, and evaluate their efforts, it will be difficult for the services and their major commands to systematically plan and implement antiterrorism programs or assess their progress in reducing the likelihood and impact of terrorist attacks. It is crucial that the services identify and support those efforts that are most likely to achieve long-term antiterrorism

goals because funding is not sufficient to eliminate or mitigate all identified vulnerabilities.

Services Are Implementing Risk Management but Provide Inadequate Oversight

The services and commands we reviewed are generally following prescribed guidance and regulations to use the DOD risk management approach in developing their installation antiterrorism requirements, but a significant weakness exists with the oversight of this process. Specifically, the services are not required to evaluate the thoroughness of all installations' annual risk management assessments or whether installations used required methodologies to perform these assessments. As previously discussed, under DOD's antiterrorism approach, three assessments (threat, vulnerability, and criticality) provide the installation commanders with the information necessary to manage the risk of a terrorist attack, and develop an antiterrorism program for the installation.[13] It also provides guidance for completing these assessments;[14] and it requires the military Departments, through the services, to oversee the antiterrorism efforts at their installations.[15] In their oversight role, the military Departments, through the services, are required to ensure that installation antiterrorism efforts adhere to the antiterrorism standards established by DOD.[16]

To implement DOD's required risk management approach, the services have issued supplements to DOD's guidance requiring installations to conduct the three risk management assessments and indicating how these assessments should be performed. The supplemental guidance of three of the services—the Army, Air Force, and the Marine Corps—requires service-specific methodologies to be used for the assessments.[17] The commands, to which the services have delegated some oversight responsibility for installations' antiterrorism efforts, generally verified that installations completed annual threat, vulnerability, and asset criticality assessments. Command officials indicated that they verify whether

[13] DOD Instruction 2000.16, para. E3.1.1.15 also calls for an assessment of incident deterrence and response capabilities.

[14] See DOD Handbook O-2000.12-H, para. E3.1.1.5, E3.1.1.15, and E3.1.1.15.4.

[15] See DOD Directive 2000.12, para. 5.9.

[16] See DOD Directive 2000.12, para. 5.9.12.

[17] Toward the end of our review, the Marine Corps issued instructions on how installations are to perform their assessments.

installations' annual risk assessments have been completed in one of two ways: (1) through the request for and receipt of copies of the written assessments or (2) through verbal verification from the installation commanders. The Navy, however, does not require that annual vulnerability assessments be documented and does not verify that these assessments are completed.

To provide oversight of the risk management process, DOD's antiterrorism standards require a higher headquarters review of subordinate installations' antiterrorism programs once every 3 years for installations that meet specific criteria.[18] These reviews are conducted by teams of specialists skilled in various disciplines (such as engineering, intelligence, and security) from the Joint Staff, service headquarters, or major command. The reviews assess, among other things, an installation's antiterrorism plans, physical security, vulnerabilities and solutions for enhanced protection, and incident response measures. These reviews, however, do not routinely evaluate the methodology used to develop the annual installation assessments.[19] Moreover, there is no requirement to review the antiterrorism programs of installations that do not meet DOD's criteria for higher headquarters assessments.

Because the results of assessments form the foundation of installation antiterrorism plans, which drive servicewide requirements, it is critical that assessments be performed consistently across each service to ensure that assessment results are comparable. According to DOD officials, installations' risk assessments were not evaluated for two reasons. First, DOD does not specifically require the services and their commands to evaluate installation assessments. Second, several command officials indicated that evaluating assessment methodologies would provide little or no added value to the process.

The Air Force and the Navy have initiatives under way that will place a greater emphasis and importance on the results of the installations' risk management efforts. Both services are using to varying degrees an automated risk management program that should improve visibility over

[18] DOD Instruction 2000.16 requires a service-level review of DOD facilities with (1) at least 300 personnel, (2) an emergency response and physical security mission, or (3) contact with local nonmilitary or foreign agencies at least once every 3 years.

[19] In technical comments provided by the Air Force, officials stated that Air Force higher headquarters reviews also include a review of annual installation assessments.

installation assessments and the resulting antiterrorism requirements. This program—the Vulnerability Assessment Management Program—will enable service and command officials to track assessment results and prioritize corrective actions servicewide.[20] The program will contain information about installations' antiterrorism requirements and the threat, vulnerability, and asset criticality assessments that support these requirements. It is also designed to allow service officials to conduct trend analyses, identify common vulnerabilities, and track corrective actions. Service officials stated that this program will also enable them to evaluate the risk assessment methodologies used at each installation, but it is unclear how this will be accomplished.

If installations' risk assessments are not periodically evaluated to ensure that assessments are complete and that a consistent or compatible methodology has been applied, then commands have no assurance that their installations' antiterrorism requirements are comparable or based on the application of risk management principles. Consequently, when the services and commands consolidate their antiterrorism requirements (through the process of merging and reprioritizing the requirements of their multiple installations), the result may not accurately reflect the services' most pressing needs. For example, if a standard methodology is not consistently applied, then vulnerabilities may not be identified and critical facilities may be overlooked. Or in the case of the Navy, the lack of assessment documentation further limits the command's ability to perform its oversight responsibility.

DOD's Combating Terrorism Funding Reports Do Not Clearly Reflect Costs

DOD has reported that $32.1 billion has been allocated or requested for combating terrorism activities from fiscal year 1999 through fiscal year 2003; however, these reported amounts may not present a clear picture of total combating terrorism costs. Each year, DOD is required to provide Congress with a report on the funds allocated to combat terrorism activities.[21] DOD's reported annual combating terrorism allocations have risen from $4.5 billion in fiscal year 1999 to $10 billion in the fiscal year 2003 budget request. Significant uncertainty exists, however, regarding the accuracy of these reported amounts because over half are associated with

[20] Both the Air Force and the Navy are requiring their installations to submit antiterrorism requirements for fiscal year 2003 in the format prescribed by the Vulnerability Assessment Management Program.

[21] 10 U.S.C. sec. 229.

personnel who may or may not be engaged in combating terrorism activities full-time.

DOD Is Required to Report Its Funding Requirements Annually

The National Defense Authorization Act for Fiscal Year 2000 requires DOD to provide Congress with an annual consolidated budget justification display that includes all of its combating terrorism activities and programs and the associated funding.[22] In response, DOD has submitted a separate budget report for fiscal years 2001, 2002, and 2003 that portrays its allocation of funds within the four categories of combating terrorism: antiterrorism/force protection, counterterrorism, consequence management, and intelligence support. The most recent budget report, submitted to Congress in March 2002, includes the following: the combating terrorism program descriptions and budget request estimates for fiscal year 2003, the estimated budget for fiscal year 2002, and the actual obligations for fiscal year 2001. It also reflects the funding provided by the Defense Emergency Response Fund[23] for fiscal years 2001 and 2002.[24]

Funding for Combating Terrorism Activities More Than Double Over 5-Year Period

If Congress passes the fiscal year 2003 budget request as submitted, annual funding to combat terrorism will increase 122 percent from fiscal year 1999 through fiscal year 2003[25]—rising from $4.5 billion (actual obligations) to $10 billion (budget request), including the Defense Emergency Response Fund request for fiscal year 2003. (See fig. 1.) In total, DOD reports that $32.1 billion has been allocated for combating terrorism activities during this 5-year period. The dollar amounts shown in figure 1 do not include funding for the current global war on terrorism, such as military operations in Afghanistan, because these activities are not intended to be included.

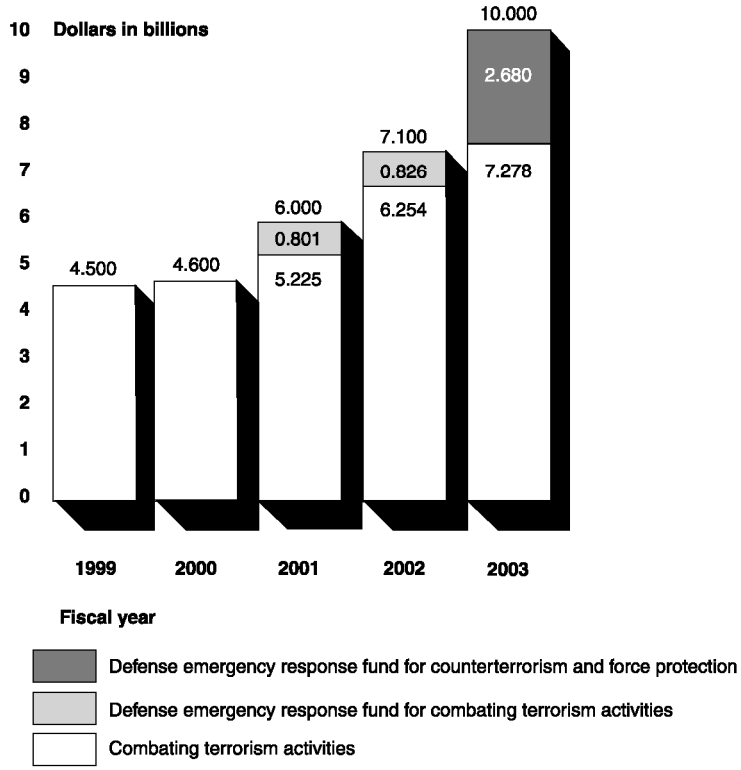
[22] P.L. 106-65, sec. 932, Oct. 5, 1999; 10 U.S.C. sec. 229.

[23] The Defense Emergency Response Fund is DOD's portion of the Emergency Supplemental Appropriations of September 2001, which was approved immediately following the attacks on the World Trade Center and the Pentagon.

[24] The Defense Emergency Response Fund request for fiscal year 2003 was provided to Congress in a separate budget justification book.

[25] In terms of fiscal year 2002 dollars, which adjusts for inflation, this increase would be 105 percent.

Figure 1: DOD's Combating Terrorism Funding for Fiscal Years 1999 to 2003



Source: GAO's analysis of DOD's combating terrorism budget reports.

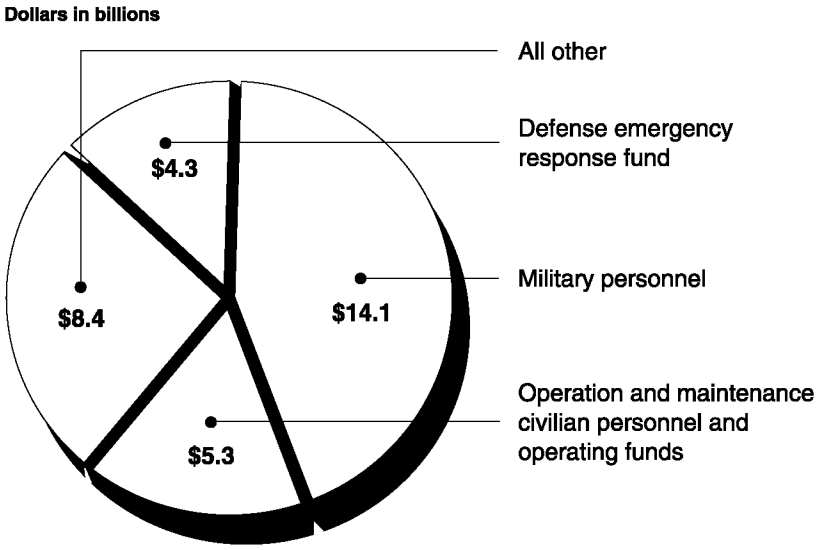
Reported Combating Terrorism Funding May Be Overstated

Although not clearly identified in DOD's budget reports, our analysis estimates that $19.4 billion (60 percent) of the $32.1 billion combating terrorism funding is for military ($14.1 billion) and civilian personnel and personnel-related operating costs ($5.3 billion); however, this estimate may be overstated. (See fig. 2.) In accordance with DOD's Financial Management Regulation,[26] the Department's combating terrorism costs include funding for personnel in designated specialties that have combating terrorism missions, such as military police, civilian police, and security guards. The military services' accounting systems do not track the time that individuals in these specialties spend on activities related to combating terrorism; therefore, the total personnel costs are reported even if the individuals spend only a portion of their time performing combating terrorism activities. The actual proportion of time these

[26] DOD 7000.14-R, Vol. 2B, Ch. 19, June 2000.

personnel spend between combating terrorism and unrelated activities (such as counter drug investigations) varies, although all of these personnel are available to perform combating terrorism duties when needed.

Figure 2: Estimated Personnel Costs as Part of Combating Terrorism Funding for Fiscal Years 1999 to 2003



Source: GAO's analysis of DOD's combating terrorism budget reports.

The $19.4 billion of estimated combating terrorism personnel costs shown in figure 2 consists of military personnel costs of $14.1 billion and estimated operation and maintenance civilian personnel costs of $5.3 billion. Other components of the total $32 billion shown include $4.3 billion from the Defense Emergency Response Fund and $8.4 billion in other appropriations, including procurement, research and development, and military construction.

Officials in the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict recognize that improvements could be made in the budget report for next year and plan to consider ways to restructure its contents to include more summary information.

Conclusions

Funding for antiterrorism requirements has increased since fiscal year 1999, but it is widely recognized that vulnerabilities at military installations will continue to outpace available funding. It is therefore essential that

funds be spent efficiently and effectively if the services are to achieve the highest level of protection possible for military personnel, equipment, and critical facilities and operations. Our analysis indicates that the military services generally are not applying a results-oriented management framework to guide their antiterrorism efforts, in part, because DOD does not yet have a Department-wide antiterrorism strategy. Without a results-oriented management framework to implement antiterrorism efforts and monitor results, the services, military commanders, and Congress will not be able to determine if past and future resources—which have been significantly increased—are achieving their desired results in the most efficient and effective manner.

The services and commands we reviewed are adhering to prescribed policies and procedures and taking significant steps to improve their capability to use a risk management approach. We identified a significant weakness in the services' current risk management approach, however, which limits their ability to ensure that these methodologies are consistently used. As a result, there is limited assurance that assessment results—which ultimately drive funding allocations—have been achieved through a consistent assessment process prescribed by DOD guidance. This creates the potential that limited resources could be misapplied and important opportunities to improve an installation's force protection posture could be overlooked.

The Department's annual combating terrorism report to Congress provides a detailed description of DOD funds allocated for combating terrorism activities, but that report should be viewed with caution because over half of the reported amounts are estimates that do not reflect actual activities dedicated to combating terrorism. Consequently, as Congress considers DOD's budget requests and oversees DOD's combating terrorism activities, it may not have a clear picture of total costs incurred by DOD for this purpose.

Recommendations for Executive Action

Because of the magnitude of the funds being allocated for, and the importance of antiterrorism efforts within, DOD, we recommend that simultaneous steps be taken within the Department to improve the management framework guiding these efforts. Accordingly, to establish a foundation for the services' antiterrorism efforts, we recommend that the Secretary of Defense (1) direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to accelerate and set a target date to issue a Department-wide antiterrorism strategy that will underpin each service's efforts, and (2) work with each service to ensure that its management framework is consistent with this Department-wide strategy.

To improve the effectiveness of the services' antiterrorism efforts, we recommend that the Secretary of Defense direct the Secretaries of the Army, Navy, and Air Force to adopt and effectively communicate a results-oriented management framework, consistent with DOD's overall antiterrorism strategy, to guide each service's antiterrorism efforts. This framework should include the following:

A strategy that defines

- long-term antiterrorism goals,
- approaches to achieve the goals, and
- key factors that might significantly affect achieving the goals.

An implementation approach that provides

- performance goals that are objective, quantifiable, and measurable;
- resources to achieve the goals;
- performance indicators to measure outputs;
- an evaluation plan to compare program results with established goals; and
- actions needed to address any unmet goals.

To improve their risk management approach for identifying antiterrorism requirements, we recommend that the Secretary of Defense direct the Secretaries of the Army, Navy, and Air Force to require

- installation commanders to document all threat, vulnerability, and asset criticality assessments and

- periodic higher headquarters evaluations of the methodologies used by installations to conduct their threat, vulnerability, and asset criticality assessments. Such an evaluation may be incorporated into the existing

service-level review process; however, for those installations that are not covered by this process, the services should develop an alternative approach.

To clarify the annual consolidated budget justification display for combating terrorism reported to Congress, we recommend that the Secretary of Defense highlight the military and civilian personnel funding included in the report and clearly indicate that these total personnel funds are reported even though the individuals may spend only a portion of their time performing combating terrorism activities.

Agency Comments and Our Evaluation

DOD agreed with all of our recommendations and stated that it is accelerating the development of an antiterrorism strategy and working with the military services to ensure that a consistent approach is followed across the Department. In commenting on this report, DOD said that it would publish an antiterrorism strategic plan by January 2003 that articulates strategic goals, objectives, and an approach to achieve them. Moreover, DOD will require each service to develop its own antiterrorism strategic plan that complements and supports the Department's plan. DOD also agreed to improve its risk management process for establishing antiterrorism requirements. In its comments, DOD said that it is revising guidance to validate the methodologies their installations use to perform threat, vulnerability, and asset criticality assessments and the thoroughness of these three assessments as part of regularly scheduled antiterrorism program reviews. DOD agreed with our recommendation to clarify how personnel costs that appear in the Department's annual combating terrorism funding report to Congress were calculated. In its fiscal year 2004 combating terrorism funding report to Congress, DOD plans to highlight the personnel costs and the methodology used to determine them.

DOD officials also provided technical comments that we have incorporated as appropriate. DOD's written comments are reprinted in their entirety in appendix II.

We are sending copies of this report to the Secretaries of Defense, the Army, the Navy, and the Air Force; the Commandant of the Marine Corps; and interested congressional committees. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff has any questions about this report, please contact me at (202) 512-6020. Key contributors to this report are listed in appendix III.

Sincerely yours,

Raymond J. Decker, Director
Defense Capabilities and Management

Appendix I: Scope and Methodology

The scope of our study was limited to the antiterrorism preparedness of Department of Defense (DOD) installations in the continental United States. To perform our review, we contacted the antiterrorism offices for each of the four military services, as well as two commands within each service. We selected an active-duty command from each service that was responsible for a large number of installations and that had a key role in providing personnel and weapons systems for military operations. Additionally, we selected a reserve command from each service because they typically have smaller-sized installations than do active-duty commands; consequently, a large number of them do not receive service-level reviews of their antiterrorism efforts.[1]

To determine whether the services use a results-oriented management framework to guide their antiterrorism efforts, we met with Office of the Secretary of Defense and service headquarters and command antiterrorism officials, and reviewed their strategic-planning documents for evidence of the critical elements of a strategic plan and performance plan—as embodied in the Government Performance and Results Act of 1993. We also reviewed service- and command-specific documents, such as campaign plans, operating orders, and briefing slides, which describe and communicate the management structure of the services and commands antiterrorism programs. We interviewed officials and gathered relevant documentation for our review primarily from the following DOD organizations located in the Washington, D.C., area:

- Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict.
- Headquarters, Department of the Army, Force Protection and Law Enforcement Division, Antiterrorism Branch.
- Headquarters, Department of the Navy, Interagency Support and Antiterrorism/ Force Protection Division.
- Headquarters, Department of the Air Force, Force Protection Branch, Directorate of Security Forces.
- Headquarters, U.S. Marine Corps, Homeland Defense Branch, Security Division.

[1] DOD Instruction 2000.16 requires facilities with (1) at least 300 personnel, (2) an emergency response and physical security mission, or (3) contact with local nonmilitary or foreign agencies to receive a service-level review at least once every 3 years.

We also spoke with officials from the following commands, who provided data on the number of domestic installations within their respective commands.

- Army Forces Command, Atlanta, Georgia (number of installations = 11).
- Navy Atlantic Fleet, Norfolk, Virginia (number of installations = 18).
- Air Combat Command, Hampton, Virginia (number of installations = 16).
- Marine Forces Atlantic, Norfolk, Virginia (number of installations = 7).
- Army National Guard, Arlington, Virginia (number of installations = 165).
- Naval Reserve Force, New Orleans, Louisiana (number of installations = 116).
- Air National Guard, Arlington, Virginia (number of installations = 69).
- Marine Force Reserve, New Orleans, Louisiana (number of installations = 42).

To determine the extent to which the military services use risk management analysis to develop antiterrorism requirements, we obtained relevant documents and interviewed antiterrorism officials from the organizations and commands previously listed as well as the following organizations:

- Joint Staff Directorate for Combating Terrorism Programs and Requirements, Washington, D.C.
- Air Force Security Forces Center, Lackland Air Force Base, San Antonio, Texas.

We reviewed DOD as well as Joint Staff-, service-, and command-specific regulations, orders, pamphlets, manuals, and other antiterrorism guidance to determine whether organizations were required to perform the three assessments (of threat, vulnerability, and asset criticality) that comprise risk management to identify and prioritize antiterrorism requirements. We also reviewed these documents for procedures and directions on how these assessments are to be performed. We spoke with headquarters and command officials about their involvement in overseeing how installations identify antiterrorism requirements and about their process for merging, reprioritizing, and funding these installation requirements. Additionally, we spoke with Air Force and Navy headquarters officials as well as officials from the Air Force Security Forces Center about the utility of the Vulnerability Assessment Management Program for prioritizing and tracking installation antiterrorism requirements servicewide.

To identify funding trends and determine if DOD accurately and completely reports its combating terrorism funding to Congress, we

obtained and analyzed the three annual combating terrorism activities budget reports that cover fiscal years 1999 through 2003. We did not independently verify the information contained in the funding reports, although we did examine the methodology and assumptions that were used to develop the information. We discussed how the budget report is reviewed and consolidated with officials from the DOD Comptroller's Office, the Office for Special Operations and Low-Intensity Conflict, and the Program Analysis and Evaluation Directorate. To determine if the military services' funding information is accurate and complete, we interviewed budget officials responsible for compiling the information for each service.

To estimate the combating terrorism personnel funding that appears in figure 2, we analyzed 5 fiscal years of funding from the previously mentioned combating terrorism budget reports. The $14.1 billion of military personnel presented in the figure represents appropriations for military personnel for combating terrorism. We estimated civilian personnel funding by combining the four antiterrorism activities that contain most of the operation and maintenance funds for personnel: physical security management and planning, security forces and technicians, law enforcement, and security and investigative matters. DOD's budget report does not distinguish civilian personnel funds from the other funds contained in these activities; therefore, our estimate of civilian personnel funds includes the nonpersonnel funds as well. However, we believe that the estimate is appropriate on the basis of our analysis of DOD's budget report and discussions with DOD officials. We could not determine the civilian personnel funds embedded in other operation and maintenance activities and in research and development activities and, therefore, did not include them in our estimate of personnel funding.

We conducted our review from February 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 22 2002

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

Dear Mr. Decker:

This is the Department of Defense (DOD) response to the General Accounting Office (GAO) draft report GAO-03-14, "COMBATING TERRORISM: Actions Needed to Guide Services' Antiterrorism Efforts at Installations," dated November 2002 (GAO Code 350084).

The Department concurs with the draft report. Comments on the recommendations are included in the enclosure. Technical and factual comments have been forwarded to your staff for consideration and inclusion into the report, as appropriate.

Sincerely,

Marshall Billingslea
Principal Deputy

Enclosure
As stated

GAO DRAFT REPORT – DATED NOVEMBER 2002
GAO-03-14 / CODE 350084

"COMBATING TERRORISM: Actions Needed to Guide Services' Antiterrorism Efforts at Installations"

DEPARTMENT OF DEFENSE RESPONSE TO THE RECOMMENDATIONS

RECOMMENDATION 1: Because of the magnitude of the funds being allocated for, and the importance of antiterrorism efforts within, DoD, GAO recommends that simultaneous steps be taken within the Department to improve the management framework guiding these efforts. Accordingly, to establish a foundation for the Services' antiterrorism efforts, GAO recommends that the Secretary of Defense (1) direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to accelerate and set a target date to issue a department-wide antiterrorism strategy that will underpin each Service's efforts, and (2) work with each Service to ensure that its management framework is consistent with this department-wide strategy. (pp. 16-17/GAO Draft Report)

DoD RESPONSE: Concur. OASD(SO/LIC) has completed the draft of the Department of Defense Antiterrorism Strategic Plan to guide DoD's antiterrorism program efforts by articulating strategic goals, objectives, and a proposed strategy to achieve them. This plan will serve as strategic guidance for all DoD Component antiterrorism programs. OASD(SO/LIC) will publish the plan no later than January 2003. OASD(SO/LIC) will orchestrate the implementation of the strategic goals and objectives throughout DoD in coordination with other OSD offices, the Joint Staff, the Services, and DoD agencies.

RECOMMENDATION 2: To improve the effectiveness of the Services' antiterrorism efforts, the GAO recommends that the Secretary of Defense direct the Secretaries of the Army, Navy, and Air Force to adopt and effectively communicate a results-oriented management framework, consistent with DoD's overall antiterrorism strategy, to guide each Service's antiterrorism efforts. This framework should include the following:

A strategy that defines
- long-term antiterrorism goals,
- approaches to achieve the goals, and
- key factors that might significantly affect achieving the goals

An implementation approach that provides
- performance goals that are objective, quantifiable, and measurable;
- resources to achieve the goals;
- performance indicators to measure outputs;
- an evaluation plan to compare program results with established goals; and
- actions needed to address any unmet goals. (p. 17/GAO Draft Report)

DoD RESPONSE: Concur with comments. DoD Directive 2000.12 is currently being revised to require the Secretaries of the Military Departments to develop Service-oriented Antiterrorism Strategic Plans that detail the vision, mission, goals, and performance measures in support of the DoD Strategic Plan. The Vulnerability Assessment Management Program is one management framework tool being used to guide Commanders in implementing performance goals.

RECOMMENDATION 3: To improve risk management approach for identifying antiterrorism requirements, GAO recommends that the Secretary of Defense direct the Secretaries of the Army, Navy, and Air Force to require

- installation commanders to document all threat, vulnerability, and asset criticality assessments and
- periodic higher headquarters evaluations of the methodologies used by installations to conduct their threat, vulnerability, and asset criticality assessments. Such an evaluation may be incorporated into the existing service-level review process; however, for those installations that are not covered by this process, the Services should develop an alternative approach. (p. 17/GAO Draft Report)

DoD RESPONSE: Concur with comments. DoD Instruction 2000.16, Standard 20, requires Commanders at all levels to review their own antiterrorism program and plans, and the program of their immediate subordinate in the chain of command, at least annually. DoD Directive 2000.12 is currently being revised to require the Secretaries of the Military Departments to ensure all installations and activities conduct comprehensive antiterrorism program reviews and assessments in accordance with DoD Instruction 2000.16. The Directive will also require Services to ensure antiterrorism program reviews include an evaluation of the Risk Management process to validate the methodology and thoroughness of assessments conducted for critical assets, terrorist threat, and vulnerabilities.

RECOMMENDATION 4: To clarify the annual consolidated budget justification display for combating terrorism reported to Congress, the GAO recommends that the Secretary of Defense highlight the military and civilian personnel funding included in the report and clearly indicate that these total personnel funds are reported even though the individuals may spend only a portion of their time performing combating terrorism activities. (p. 18/GAO Draft Report)

DoD RESPONSE: Concur. The Fiscal Year 2004 consolidated budget justification display for combating terrorism activities will be annotated to highlight the personnel costs and the methodology used to determine the military and civilian personnel costs associated with combating terrorism activities.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Ray Decker, (202) 512-6020
Bob Repasky, (202) 512-9868

Acknowledgments

In addition to those named above, Alan Byroade, J. Paul Newton, Marc Schwartz, Corinna Wengryn, R. K. Wild, Susan Woodward, and Richard Yeh made key contributions to this report.

Related GAO Products

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

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: 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. Washington, D.C.: 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.

Combating Terrorism: Comments on Counterterrorism Leadership and National Strategy. GAO-01-556T. Washington, D.C.: March 27, 2001.

Combating Terrorism: Linking Threats to Strategies and Resources. GAO/T-NSIAD-00-218. Washington, D.C.: July 26, 2000.

Combating Terrorism: Action Taken but Considerable Risks Remain for Forces Overseas. GAO/NSIAD-00-181. Washington, D.C.: July 19, 2000).

Chemical and Biological Defense: Program Planning and Evaluation Should Follow Results Act Framework. GAO/T-NSIAD-00-180. Washington, D.C.: May 24, 2000.

Chemical and Biological Defense: Observations on Actions Taken to Protect Military Forces. GAO/T-NSIAD-00-49. Washington, D.C.: October 20, 1999.

Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences. GAO/AIMD-00-1. Washington, D.C.: October 1, 1999.

Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks. GAO/NSIAD-99-163. Washington, D.C.: September 7, 1999.

Combating Terrorism: Opportunities to Improve Domestic Preparedness Program Focus and Efficiency. GAO/NSIAD-99-3. Washington, D.C.: November 12, 1998.

Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments. GAO/NSIAD-98-74. Washington, D.C.: April 9, 1998.

Combating Terrorism: Efforts to Protect U.S. Forces in Turkey and the Middle East. GAO/T-NSIAD-98-44. Washington, D.C.: October 28, 1997.

Combating Terrorism: Status of DOD Efforts to Protect Its Forces Overseas. GAO/NSIAD-97-207. Washington, D.C.: July 21, 1997.

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