United States General Accounting Office

GAO

Report to the Ranking Minority Member, Committee on Armed Services, House of Representatives

July 2000

COMBATING TERRORISM

Action Taken but Considerable Risks Remain for Forces Overseas

GAO/NSIAD-00-181

Contents

Abbreviations

DOD	Department of Defense
AT/FP	antiterrorism/force protection

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

National Security and
International Affairs Division

B-285538

July 19, 2000

The Honorable Ike Skelton
Ranking Minority Member
Committee on Armed Services
House of Representatives

Dear Mr. Skelton:

In November 1995, a car bomb exploded in Riyadh, Saudi Arabia, killing five Americans. In June 1996, terrorists attacked the U.S. military complex at Khobar Towers in Saudi Arabia, killing 19 Americans and wounding hundreds more. In September of that year, the Secretary of Defense named the Chairman of the Joint Chiefs of Staff as his principal advisor on antiterrorism/force protection.[1] The Chairman later announced his goal that the Department of Defense (DOD) would become the recognized leader in antiterrorism/force protection throughout the world. Even though a terrorist attack has not occurred at a U.S. military installation since Khobar Towers, protecting U.S. forces against terrorism remains a top DOD priority. In late 1996 through June 1997, we evaluated DOD's efforts to protect U.S. forces stationed overseas from terrorist attacks. We reported that DOD had not taken the steps necessary to promote a comprehensive, consistent approach to antiterrorism that would give commanders at all levels the tools they needed to fulfill their antiterrorism responsibilities.[2] In addition, we noted that (1) DOD lacked prescriptive, measurable physical security standards to determine whether antiterrorism measures were sufficient; (2) DOD lacked assurances that the antiterrorism programs implemented by local commanders met a consistent minimum standard for all overseas personnel; and (3) many U.S. military personnel stationed overseas were not specifically covered by the antiterrorism plans

[1]DOD's antiterrorism/force protection program seeks to (1) reduce the likelihood that DOD-affiliated personnel, their families, facilities, and materiel will be subject to a terrorist attack and (2) mitigate the effects of such attacks should they occur.

[2]*Combating Terrorism: Status of DOD Efforts to Protect Its Forces Overseas* (GAO/NSIAD-97-207, July 21, 1997).

of either the geographic combatant commander[3] or a country's State Department representative (e.g., U.S. ambassador or chief of mission). We made several recommendations to the Secretary of Defense that were directed toward developing common standards and procedures and to ensuring that security responsibility for all DOD personnel overseas was clear.

As you requested, we evaluated DOD's efforts since our last report to improve its antiterrorism/force protection program. This report discusses

- the extent to which DOD has made improvements to its antiterrorism/force protection program overseas,
- changes in DOD's process for assessing and reporting vulnerabilities at overseas installations, and
- the adequacy of antiterrorism/force protection funding and staff.

To conduct this work, we visited 19 sites in Europe, the Middle East, and the Pacific. We also visited four of the five geographic combatant commands as well as most of the service commands in Europe, the Middle East, and the Pacific. We are not discussing installation specific information in this report for security reasons. Our scope and methodology are in appendix I.

Results in Brief

Overall, military forces stationed overseas are better protected today than they were 3 years ago. The Joint Staff has developed DOD-wide construction standards to ensure that antiterrorism/force protection measures are included in new construction. In addition, DOD has signed agreements with the Department of State and U.S. ambassadors or chiefs of mission to protect DOD personnel not under the jurisdiction of commanders. Geographic combatant commands have created permanent antiterrorism/force protection offices, hired permanent antiterrorism/force protection staff, and developed systems to monitor progress to correct vulnerabilities. Installation commanders are more aware of their responsibility to protect their forces from terrorist attack and, despite

[3]Operational control of the U.S. combat forces is assigned to the nation's Unified Combatant Commands. A Unified Combatant Command is composed of forces from two or more services, has a broad and continuing mission, and is normally organized on a geographical basis. The five geographic combatant commands are the Central Command, European Command, Pacific Command, Southern Command, and Joint Forces Command.

funding constraints, have addressed many security vulnerabilities. However, significant security and procedural antiterrorism/force protection problems continue at many installations. For example, some installations have not developed plans to deal with terrorist attacks, others have no effective means of stopping unauthorized vehicles from entering the installation, and some lack secure access to important intelligence information.

Commanders are better able to determine their vulnerability to terrorist attacks than when we last reported. Vulnerability assessments are now being conducted more routinely and are based on a defined set of criteria. However, vulnerability assessment reports do not provide specific actions to rectify problems mentioned in the reports. Additionally, there is no comprehensive method in place to share solutions to common problems among different installations.

Limited antiterrorism funding and trained staff have affected the ability of commanders to correct known vulnerabilities. Funding for antiterrorism protection has been, and will likely continue to be, significantly less than what installation and geographic combatant commanders have determined they require, despite the fact that senior DOD leaders have designated antiterrorism/force protection as a high priority item. For example, some overseas service commands have repeatedly received less than 50 percent of the money the commands believe they require to correct or mitigate vulnerabilities. According to antiterrorism/force protection managers, this level of funding has limited their ability to address vulnerabilities. Congress requires DOD to provide information on proposed antiterrorism/force protection funding and projects as part of its consolidated combating terrorism budget submission; however, it does not require DOD to provide information on the number of projects that remain to be funded. Without information on the types of projects that need funding, Congress does not have an accurate picture of the extent of the risk that U.S. forces face from terrorism. In addition, installations we visited did not have adequately trained personnel dedicated to managing and implementing antiterrorism solutions.

We are making recommendations to improve the vulnerability assessment reporting process, increase congressional visibility of unfunded antiterrorism/force protection projects to correct or mitigate vulnerabilities, and improve the training program for antiterrorism/force protection managers. In written comments to our draft report, the Department of Defense agreed with our recommendations to improve the

vulnerability assessment reporting process and the training program for antiterrorism/force protection managers. The Department disagreed with our recommendation to increase congressional visibility of unfunded projects that would correct or mitigate vulnerabilities because it believes that the current planning, programming, and budgeting system is effective and ensures that high priority items are funded. Despite the Department's position, we believe this information would enhance congressional oversight and make Congress more aware of the types of risk that servicemembers face every day. As a result, we have added a matter for congressional consideration that would require the Department of Defense to provide Congress with detailed information on the unfunded projects.

Background

The Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict is the principal staff assistant and advisor to the Secretary of Defense for antiterrorism/force protection (AT/FP) policy. While this office focuses on policy, the Chairman of the Joint Chiefs of Staff and the Combating Terrorism directorate within the Joint Staff focus on implementing DOD's AT/FP program. The Joint Staff's responsibilities include reviewing the services' AT/FP budgets, developing standards, managing the Joint Staff Integrated Vulnerability Assessment program, and representing the geographic combatant commanders on AT/FP matters.

DOD policy makes commanders responsible for protecting their forces from terrorist attacks. For forces overseas, the responsibility rests with the geographic combatant commander and the installation commander, with the support of the service headquarters. The geographic combatant commanders are responsible for developing antiterrorism policies that apply at the installations in their areas of responsibility and that take precedence over service or other DOD component AT/FP policies. They are also responsible for determining the threat levels for each country in their area of responsibility, identifying the money and manpower needed to achieve sufficient AT/FP, and working with the services to provide the resources necessary. Finally, because all risks cannot be eliminated, the geographic combatant commanders are responsible for determining the types of risks their forces will face as they undertake their missions. Installation commanders are responsible for protecting the people, assets, and facilities under their command from terrorist attacks. The installation commander, working with the installation AT/FP manager, is responsible for ensuring that AT/FP standards established by DOD, the geographic combatant commanders, the services, and the service headquarters are implemented. Additionally, because DOD recognizes that not all

vulnerabilities can be addressed, installation commanders practice risk management—to decide what risks can be accepted and what risks are too great to be accepted. When the risk is unacceptable, the commander is responsible for taking action to mitigate the risk.

Although geographic combatant commanders have overall responsibility to protect forces assigned to them, individual services are responsible for funding an installation's AT/FP needs and for providing the required number of trained personnel. The majority of funds used for AT/FP activities (excluding the cost of military personnel) are located in the services' Operation and Maintenance appropriations. Operation and Maintenance appropriations are generally used to fund readiness activities, equipment maintenance, recruiting, pay for civilian employees (including contract security guards), and the everyday costs of running an installation. A number of subactivities within this appropriation fund specific expenses. Examples of the subactivities include real property maintenance, depot maintenance, and base operating support. The base operating support subactivity pays for expenses such as utilities, communications, security, building repair, and maintenance. Traditionally, the services have included funds for AT/FP in the base operating support subactivity, and AT/FP activities must compete against other activities for the same limited funding.

Shortly after the Khobar Towers bombing, the Secretary of Defense established the Chairman of the Joint Chiefs of Staff's Combating Terrorism Readiness Initiative Fund.[4] The Fund, which is managed by the Joint Staff, was not intended to relieve the services of their responsibility to fund AT/FP projects; rather, it was intended to provide funding for emergency or other unforeseen high-priority, combating terrorism needs. In fiscal year 2000, the Fund totaled $15 million—$10 million of Operation and Maintenance funds and $5 million of procurement funds. This level of funding is scheduled to continue through fiscal year 2002. In fiscal years 2003 through 2007, the Fund will be reduced to a total of $10 million a year according to DOD.

[4]Chairman of the Joint Chiefs of Staff Instruction 5261.01A, Aug. 1, 1998, Combating Terrorism Readiness Initiative Fund.

Commands at All Levels Have Acted to Protect Their Forces, but Challenges Remain

Since we last reported in 1997, DOD has improved its AT/FP program. Improvements have been made at the Joint Staff, the geographic combatant command, and the installation levels. Specifically, more guidance is available to help develop and implement programs; many physical security vulnerabilities have been corrected; and in cases where vulnerabilities cannot be corrected, commanders have taken actions to mitigate potential damage. Such actions included adding fragment retention film to windows, installing barriers, moving personnel into base housing, erecting fences, and moving parking lots. Although improvements in AT/FP have been made, physical security and procedural problems (i.e., a lack of personnel alerting systems and access control and AT/FP plans) continue to put U.S. forces at risk of terrorist attack.

Joint Staff Has Taken Action to Improve Antiterrorism/Force Protection

The Joint Staff has taken significant actions to improve commanders' AT/FP programs. First, in December 1999, DOD issued standards (developed under the guidance of the Joint Staff) for new construction in the first volume of the DOD Security Engineering document. The remaining two volumes are expected to be completed by December 2002. The new construction standards are minimum standards and provide guidance for design criteria, protective strategies, and the costs for protective measures against higher threats. Second, the Departments of Defense and State have signed a Memorandum of Understanding, and over 90 country-level Memorandums of Agreement have been signed between the geographic combatant commanders and their local U.S. ambassadors or chiefs of mission. These agreements clarify who is responsible for providing AT/FP to DOD personnel not under the direct command of the geographic combatant commanders. These agreements cover 75 percent of these personnel (about 7,400 people). The State Department has set a goal for completing the remaining Memorandums of Agreement by summer 2000.

The Joint Staff also administers the Chairman of the Joint Chiefs of Staff's Combating Terrorism Readiness Initiatives Fund, which has allocated over $80 million to installations in the U.S. and abroad since 1997.[5] At several locations we visited, this Fund was the installation's primary source of

[5]The Joint Staff allocated $23.94 million (including $10 million in money that became available at the end of the fiscal year) in fiscal year 1997, $35.098 million (including $20 million in money that became available at the end of the fiscal year) in fiscal year 1998, and $14.942 million in fiscal year 1999. As of March 2000, the Joint Staff had allocated $8.5 million in fiscal year 2000.

funding for AT/FP improvements. Some improvements provided by this Fund include perimeter lighting, fences, road barriers, guard shacks, and explosive detectors.

In addition, the Joint Staff has also sponsored vulnerability assessment teams and educational initiatives. The Joint Staff Integrated Vulnerability Assessment teams, which were initiated in September 1996, have completed 243 vulnerability assessments worldwide. As discussed in more detail below, these assessments bring a level of expertise, a consistent level of quality, and a standardized methodology not previously available to installation commanders. These assessment teams have also provided educational opportunities for local AT/FP managers by teaching them how to write AT/FP and weapons of mass destruction response plans. The Joint Staff has also been actively developing outreach programs, including CD-ROMs and a quarterly newsletter designed to share good AT/FP ideas and to help AT/FP managers improve their programs.

Actions Taken by Geographic Combatant Commands

The geographic combatant commanders and overseas service headquarters have also taken action to improve the management of their AT/FP programs. U.S. Southern Command and U.S. Forces Korea have established full-time AT/FP offices and designated full-time AT/FP staffs since our last review. Military force structure limitations and continuity problems (due to personnel rotations) are being addressed at U.S. Army Europe and the 8th Army in Korea through the creation of full-time civilian AT/FP positions. Three geographic combatant commands—U.S. European Command, U.S. Southern Command, and U.S. Central Command—have developed vulnerability monitoring systems that help commanders to be aware of vulnerabilities and to monitor progress toward resolution of issues identified by vulnerability assessments. In addition, recognizing a need for additional training for AT/FP managers, U.S. European Command developed a 5-day course to introduce AT/FP managers to a variety of aspects of the AT/FP program. Finally, all of the geographic combatant commands we visited now have command-specific construction standards. At the time of our last report, only the Central Command had developed construction standards.

Installation Commanders' Actions

Installation commanders have made progress in institutionalizing AT/FP programs, increasing AT/FP awareness, and reducing physical security vulnerabilities. Commanders at all the installations we visited had designated AT/FP program managers. Also, every installation we visited

had an AT/FP awareness program and in some cases, used the local armed forces cable network to convey AT/FP messages. To assist in making decisions on AT/FP priorities and funding issues, nearly all the installations we visited had established AT/FP working groups or councils.

When funding was available, commanders addressed vulnerabilities. When vulnerabilities could not be fully addressed, commanders took action to mitigate the potential damage from a terrorist attack. Some of the actions have included increasing surveillance of the road, closing gates, and better protecting the people in buildings by applying fragment retention film to the windows and moving people away from the vulnerable side of the building.

Notwithstanding Progress, Problems Remain

Notwithstanding improvements, significant physical security and procedural AT/FP problems remain at many installations. The problems we observed during our installation visits included physical security and procedural issues. The Joint Staff's vulnerability assessments at 93 installations in 1999 found many of the same problems we observed. Some of these problems are described below:

- Poor installation AT/FP planning. Some installations we visited in the U.S. European Command and the U.S. Pacific Command had not completed their AT/FP installation plans almost 3 years after DOD established this requirement. The Joint Staff assessments identified poor or nonexistent AT/FP planning at many installations and further noted that some installations had AT/FP plans, but did not exercise them as required by DOD instruction. Planning is imperative so that all personnel will know what to do and how to react in any given situation. Recently, the Chairman of the Joint Chiefs of Staff reaffirmed the importance of AT/FP planning in a message to the geographic combatant commanders and the service chiefs.
- Lack of access control. Some of the installations we visited in the U.S. Pacific Command had no gates and/or no effective means of stopping unauthorized vehicles from entering the facility. We were told of one instance where a pizza delivery vehicle drove onto base without stopping because the driver failed to realize he was entering the base. The AT/FP manager at one large installation told us that a barrier system designed to stop cars was broken and that there were no plans to fix it because it was not cost-effective to keep it in working order in cold weather. The Joint Staff compilation report also noted that barriers at installation main gates were either nonexistent or poorly placed and

that installation perimeter gates did not have an effective means of preventing a high-speed vehicle approach. The report also noted that vehicle access controls at the gates were inefficient, inconsistent, or nonexistent; in many instances, installations lacked vehicle inspection equipment and guards either were unaware of control procedures or did not always follow them.

- Poorly maintained or overgrown perimeter fences. At one installation in the U.S. European Command, the perimeter fence had been cut, presumably by students, to create shortcuts on and off base. In the Pacific Command, we found egregious examples of encroachment on perimeter fences in which host nation housing leaned against the perimeter wall and drainage pipes were inserted through the perimeter wall by local residents.
- Lack of personnel alerting systems. This equipment is designed to alert all personnel in a given area to terrorism and other emergencies. At least one expert believes that a properly functioning personnel alerting system would have saved lives at Khobar Towers. Personnel alerting systems were lacking at many installations we visited.
- Lack of access to timely intelligence information. Some installations were not connected to intelligence databases via secure lines, which could delay the transmission of intelligence information to AT/FP personnel. Some installations possessed one secure computer for many users and other installations had no secure computers available at the installation.
- Shortage of security forces. In one country we visited, a Navy base was forced to use sailors without a security background to meet its basic every day AT/FP responsibilities. One Air Force base we visited is routinely short of experienced security personnel because it regularly deploys security force personnel to the Middle East. Also, we found that in other countries Army intelligence personnel often deploy, leaving installations without an adequate local intelligence capability to meet AT/FP needs. This was a major vulnerability issue noted in the Joint Staff assessments as well.
- Shortage of AT/FP staff. A majority of the installation AT/FP managers we interviewed told us that they lacked sufficient AT/FP staff to complete the myriad program requirements established by DOD and the geographic combatant commanders. Approximately 66 percent of the AT/FP managers we met with have other full-time jobs and have been assigned the responsibility for AT/FP as an additional duty. One subordinate command official told us that the staff was so busy with non-AT/FP matters that they had no time to do any AT/FP planning—they simply put out AT/FP “fires.” One manager believed that

the lack of full-time AT/FP managers indicated that the service did not really place a high priority on AT/FP.

Vulnerability Assessments Have Improved, but Weaknesses Remain

Since our last report in 1997, vulnerability assessments have been conducted more routinely and have been based on a defined set of criteria. Through vulnerability assessments, DOD, the geographic combatant commands, and the services evaluate their ability to defend against a terrorist attack and highlight security weaknesses that terrorists could exploit. In 1997, vulnerability assessments differed in frequency, approach, and quality. Within DOD, commands did not have a common understanding of how to conduct a vulnerability assessment or what constituted a high quality assessment. In addition, some vulnerability assessment reports failed to provide specific information on the vulnerabilities found at installations.

This situation has improved in the last 3 years. DOD guidance now requires that all installations undergo a higher headquarters AT/FP vulnerability assessment at least once every 3 years (individual commands may elect to require more frequent assessments). At a minimum, according to DOD policy, all of these higher headquarters assessments must assess the following functional areas: (1) counterintelligence, law enforcement, and intelligence support; (2) physical security; (3) vulnerability and response to a threat; (4) force protection plans and programs; (5) host nation, local community, interservice, and tenant support; and (6) activity-specific characteristics. A Joint Staff, geographic combatant command, or service vulnerability assessment can satisfy assessment requirements. In the following paragraphs, we evaluate the vulnerability assessments conducted by these entities since our last report.

In September 1996, the Joint Staff through the Defense Threat Reduction Agency began to conduct Joint Staff Integrated Vulnerability Assessments at installations.[6] The teams conducting the assessments have since been working to identify installation vulnerabilities and present options for commanders to mitigate vulnerabilities with a focus on avoiding mass casualties. During a week long on-site assessment, the team reviews site specific plans, programs, and procedures. Areas they assess include

[6]At the time, the Defense Threat Reduction Agency was known as the Defense Special Weapons Agency. The name change, the result of a merger of four organizations, took place in October 1998.

physical security systems, guard-force procedures, incident response, structural engineering, infrastructure engineering, intelligence processes, and ability to manage the consequences of an attack. The teams compile reports outlining the various problems or vulnerabilities and make recommendations for ways to improve AT/FP. Because AT/FP is a commander's program, DOD does not require commanders to correct the vulnerabilities noted in the reports.

AT/FP personnel told us that the Joint Staff Integrated Vulnerability Assessments served to educate the command to vulnerabilities and were useful in planning projects and prioritizing them against available resources. However, some changes could make this tool even more valuable. The assessment teams have not been providing a commander with specific directions on how to deal with vulnerabilities. For example, the report may mention that the installation's windows need fragment retention film,[7] but it would not tell the commander if installing the film is more or less important than fixing other vulnerabilities, or advise the commander as to what type of film might be the best fix for the problem, nor would it outline how other installations have dealt with similar issues. In addition, some AT/FP personnel found that the reports could be more user-friendly. We were told that the reports are difficult to read and understand, too long, and poorly structured.

Additionally, other installations facing similar problems cannot take advantage of the advice provided in the assessment team's report because DOD has no formal, comprehensive mechanism to share best practices or lessons learned. This condition is particularly unfortunate for installations that are too small to receive Joint Staff-sponsored assessments or installations that independently identify vulnerabilities between assessments and could benefit from the teams' expertise secondhand.

The Joint Staff is responding to some of the commanders' and AT/FP officials' concerns. For example, Joint Service Integrated Vulnerability Assessment team leaders told us that the executive summary of future assessment reports will highlight those vulnerabilities that the team believes to be the most pressing. The vulnerabilities in the executive summary, while not in priority order, will be segmented into two categories—those that can be addressed with little or no money and those

[7]Fragment retention film is a thin, optically clear film that is applied to glass to minimize the spread of glass fragments when the glass is shattered.

that will require funding. This differentiation should make it easier for a command to take immediate action on some vulnerabilities. Additionally, an e-mail account has been established to allow (1) AT/FP managers to ask questions and (2) assessment team members to provide potential solutions to specific issues. Finally, according to Joint Staff officials, they have started to list all observations with bullet points for improved readability.

In addition to the Joint Staff-sponsored assessment teams, the geographic combatant commands and the services sponsor a number of other vulnerability assessment teams. For example, U.S. Central Command has formed the Joint Rear Area Coordinator assessment team, and U.S. Army Europe has formed teams to assess installations in their area of responsibility. Both the Air Force and the Navy have established teams, as have the Air Forces' overseas service headquarters such as the Pacific Air Force and U.S. Air Force Europe. The service- and command-level teams generally assess installations that the Joint Staff-sponsored teams do not assess.

These assessments differ in quality from the Joint Staff-sponsored assessments since these teams generally do not have the same level of expertise and tend to be inconsistent in their makeup. On the other hand, these assessments can be helpful in that the teams visit even the smallest installations and provide a unique local- or service-centered perspective.

Services Have Not Adequately Funded or Properly Staffed the Antiterrorism/Force Protection Program

Although DOD makes the geographic combatant commanders responsible for protecting U.S. forces from terrorist attack, it is up to the services to provide the necessary personnel and funding to correct vulnerabilities and upgrade facilities. Notwithstanding AT/FP's high priority status within DOD, funding for AT/FP has been, and will likely continue to be, significantly less than what installation and geographic combatant commanders feel they need to meet DOD's goals. Commanders and AT/FP program managers we met with stated that insufficient service

funding had limited their ability to meet their AT/FP responsibilities.[8] Although Congress has taken action to obtain more information about AT/FP financing, DOD is not required to provide Congress with information about unfunded AT/FP projects that would correct or mitigate vulnerabilities. In addition, DOD has not provided AT/FP managers with the training necessary to serve as AT/FP advisors to installation commanding officers.

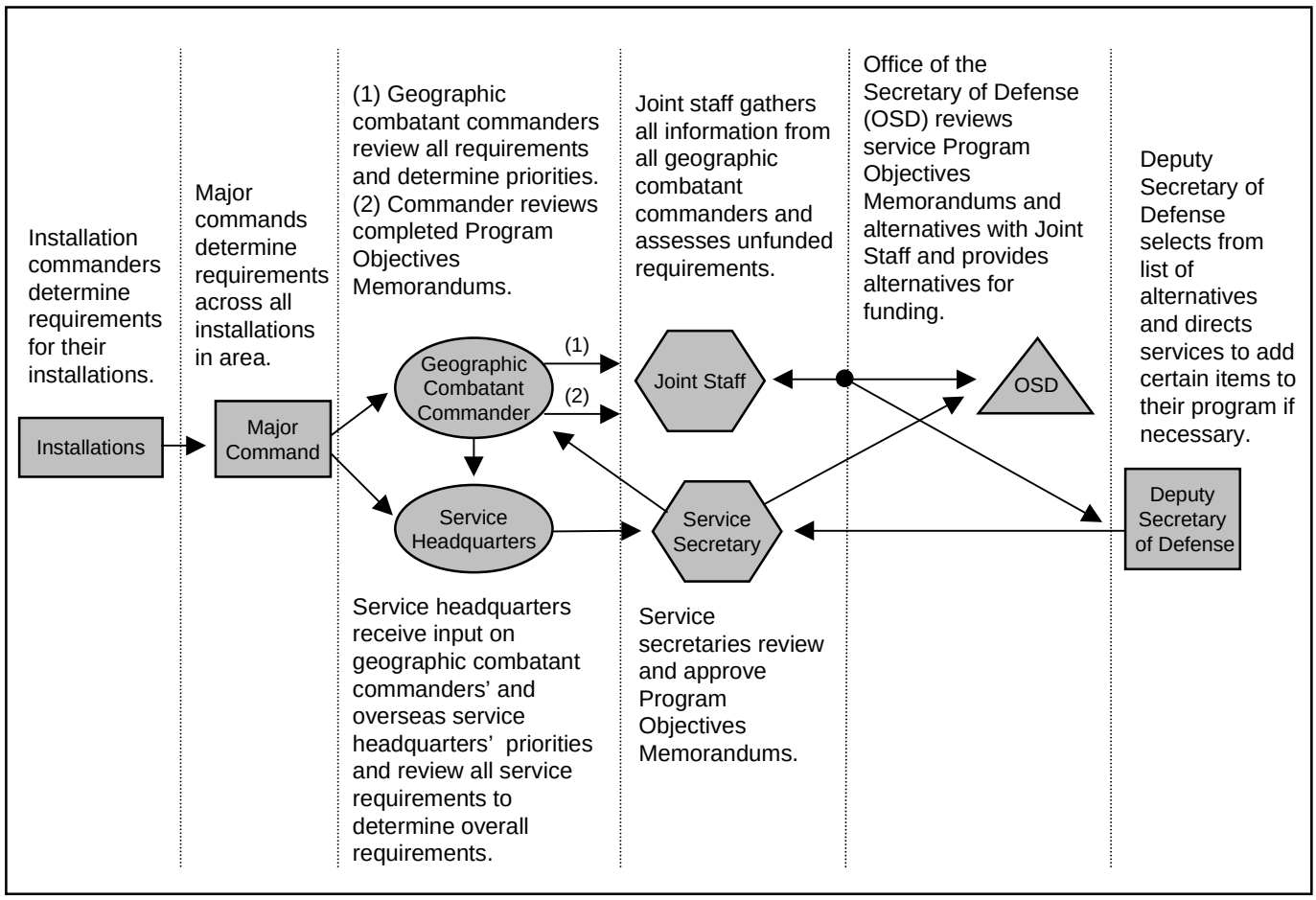
Development of the Services' Funding Plans Starts at the Installations

Every 2 years, the services develop the Program Objectives Memorandums,[9] which outline the services' spending plans for the following 6 years. The Program Objectives Memorandums are the starting point for the budget requests that are sent to Congress annually. Figure 1 details the steps in this process.

[8]We have only included data for the Pacific and European Commands because this report focuses on protecting troops overseas and the majority of U.S. troops stationed overseas are located in these two commands. The Central Command is not included because the Army and the Air Force provide no AT/FP funds for their installations in the Central Command. At those installations, AT/FP requirements are funded by host nations or funds provided by Congress for contingency operations. The Navy provides AT/FP funds for its installations in Bahrain. According to Navy Central Command officials, AT/FP funding has been sufficient to meet their AT/FP requirements. The Southern Command was excluded because of the limited number of troops it has located outside of the United States.

[9]The Program Objectives Memorandums are developed in even numbered years. At the time of our report, the services were developing the fiscal year 2002 through 2007 Program Objectives Memorandums. In the odd years, the services review the previously developed Program Objectives Memorandums to ensure that they still address the needs of the services. For example, in fiscal year 2001 the services will review their spending plans for fiscal years 2003 through 2007. In fiscal year 2001, the services will also review the fiscal year 2002 spending plan to make any necessary adjustments before submitting the plan as its budget request to Congress.

Figure 1: DOD Program Objectives Memorandum Process



Source: GAO analysis of DOD's Program Objectives Memorandum process.

As the figure shows, the process begins with an installation commander providing a prioritized list of unfunded requirements, including AT/FP requirements to the major service commands. At the services' major commands, the installations' requirements are combined, prioritized (using guidance from the service and geographic combatant commander), and forwarded to the service headquarters for consideration. At the service headquarters, AT/FP requirements compete against other requirements for funds. The service secretary approves the Program Objectives Memorandum and submits it to the Office of the Secretary of Defense for approval where subject matter experts, such as those in the Joint Staff

office responsible for AT/FP issues, review them and develop alternative funding plans. If the Deputy Secretary of Defense is convinced that the services' spending plans need to be adjusted, he will direct the services to adjust their plans. After the Program Objectives Memorandum process is completed, the budgeting phase begins with the services developing detailed budget estimates. These estimates are also reviewed by the subject matter experts, and are approved or revised by the Deputy Secretary of Defense. The budget is then finalized and sent to Congress. The Deputy Secretary of Defense has directed the services to increase AT/FP funding every year since 1996.

Past Funding Has Not Met Needs

Although we could not obtain complete funding data for all the service commands we visited, the data that is available reveals that funding for AT/FP requirements in fiscal years 1999 and 2000 has been significantly less than many commanders of overseas installations in the Pacific and Europe required,[10] as the following examples indicate:

- In fiscal years 1999 and 2000, the Pacific Air Forces received approximately 4 percent and 2 percent, respectively, of funds needed to meet their AT/FP requirements. In fiscal year 1999, $120,000 of the $3.2 million AT/FP requirement was funded. For fiscal year 2000, $52,000 was provided to meet $2.5 million of AT/FP requirements. Projects that installations deferred included improving blast protection, applying fragment retention film to windows to reduce the hazards of flying glass, and developing new AT/FP training materials.
- For fiscal year 2000, the Army in Korea needed $44.6 million for civilian gate guards and AT/FP physical security improvements and equipment. However, the Army only provided 22 percent ($9.8 million) of the requirement. According to the commanding general of the Army in Korea, without additional funding the Command will have to divert funds, including unit training money, to pay for the required guards. This diversion will result in reduced readiness. Projects to improve communications, blast protection, and access control remain undone due to a lack of funds.
- In fiscal year 1999, the U.S. Navy, Pacific Fleet received $30.3 million, or about 60 percent, of its $50.4 million requirement. In fiscal year 2000, it

[10]We did not validate the AT/FP requirements provided to us by the commands. The requirements presented in this report represent the funding that the commands believe they need to address their AT/FP vulnerabilities.

received $28.1 million, or 54 percent, of its $52 million requirement. Projects to improve base access control, lighting, and communications remained unfunded at the time of our visit.

- The Army Command in Europe was unable to provide us details about its requirements for fiscal year 1999 or 2000. However, according to documents from the Army in Europe, in both fiscal years the Army failed to provide sufficient funds to contract for all of the civilian security guards required to implement the geographic combatant commander's decision to limit access to U.S. bases in Europe.

Planned Funding for Fiscal Year 2001 Leaves Commands Underfunded Again

The services' proposed AT/FP spending plans for fiscal year 2001 left every command in the Pacific and in Europe with unfunded requirements. For example, the Army's spending plan for its forces in Europe totaled only 54 percent of its requirement, while the Air Force budget for its command in the Pacific totaled 3 percent of the requirement. Table 1 outlines the services' requirements and proposed spending plans, the resulting shortage, and the percentage of the requirement the spending plan fulfills for fiscal year 2001.

Table 1: Service AT/FP Requirement, Proposed Spending Plan, Shortage, and Percentage of Requirement Fulfilled for Fiscal Year 2001

Dollars in millions

	Army: Pacific	Navy: Pacific	Air Force: Pacific	Army: Korea	Air Force: Europe	Navy: Europe	Army: Europe	Total
Required	6.8	53.6	2.2	35.5	19.6	24.5	132.3	**274.5**
Proposed spending	6.3	27.0	0.06	12[a]	7.1[a]	17.6	71.2[a]	**141.3**
Shortage	0.5	26.6	2.1	23.5	12.5	6.9	61.1	**133.2**
Percent of requirement fulfilled	92	50	3	34	36	72	54	**51**

[a]Data does not include increases made at the direction of the Deputy Secretary of Defense after the service secretaries approved the budget proposals.

Source: Command- and service-provided data.

In August 1999, the Deputy Secretary of Defense directed the Army and the Air Force to increase the funding levels for AT/FP in fiscal year 2001. At that time, the Deputy Secretary of Defense directed (1) the Army to add $32.5 million to its AT/FP budget for Europe and $7 million to fund contract

security guards at installations in Korea and (2) the Air Force to add $12.5 million to its AT/FP budget for the U.S. Air Forces in Europe. As a result, the U.S. Air Forces in Europe's AT/FP requirements are fully funded for fiscal year 2001. Also, according to an official from the U.S. Naval Forces in Europe's AT/FP office, the AT/FP program is fully funded for fiscal year 2001 because it received contingency funds and supplemental funds in fiscal year 1999. These funds allowed the program to address some fiscal year 2001 requirements in fiscal year 1999. The remaining overseas service headquarters remain underfunded.

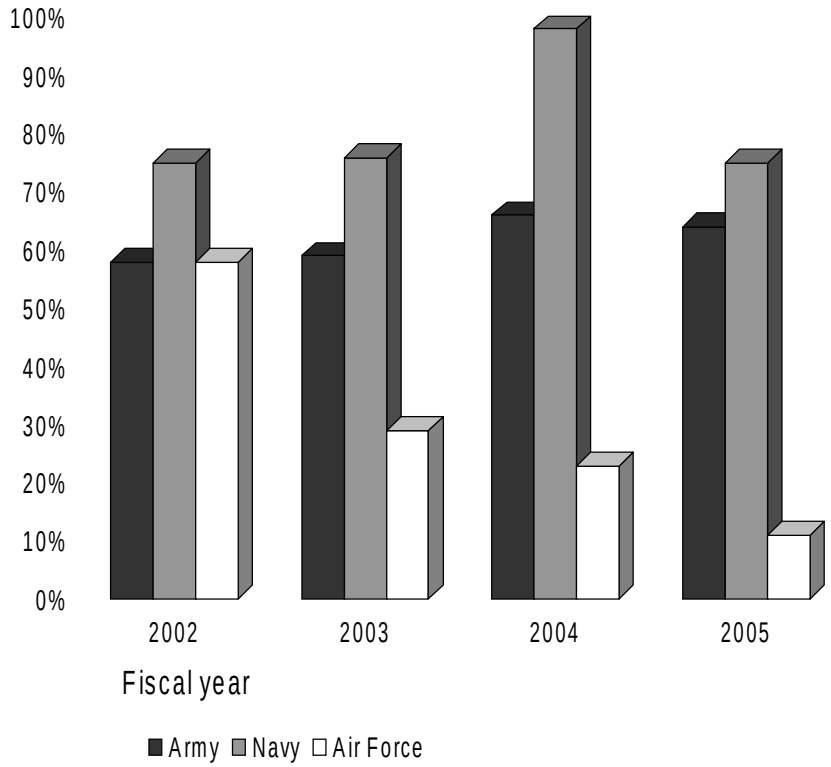
Funding for the Future Looks Bleak

The services' current funding plans for fiscal years 2002 through 2005 continue the trend of under funding AT/FP requirements. According to a document developed by the Office of the Secretary of Defense for use during the 1999 review of the services' fiscal year 2001 to 2005 Program Objectives Memorandums, the services did not provide

- funding for physical security improvements validated by vulnerability assessments,
- full funding for investments arising from establishment of AT/FP standards, or
- full funding for contract security guards.

As figures 2 and 3 show, the planned AT/FP funding for Army, Air Force, and Navy forces in Europe and the Pacific is consistently below funding requirements. The figures reflect current requirements and planned spending levels.

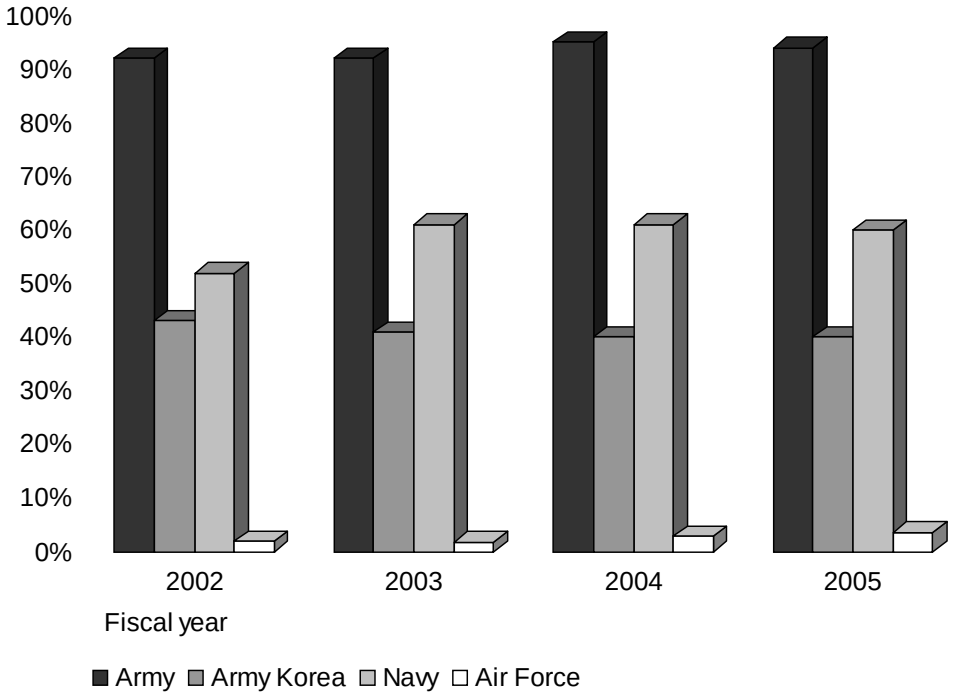
Figure 2: Percentage of Antiterrorism/Force Protection Requirement the Services Plan to Fund in the European Command



Note: Data for Army and Navy does not include military manpower. Data for the Air Force includes some military manpower.

Source: GAO's analysis of service and command data.

Figure 3: Percentage of Antiterrorism/Force Protection Funding Requirement the Services Plan to Fund in the Pacific Command



Note: Data includes operation and maintenance requirements only.

Source: GAO's analysis of service and command data.

At the time of our review, the services were updating their fiscal year 2002 through 2005 spending plans. The Joint Staff estimates that the services will need to add an additional $700 million over the current levels of spending to address AT/FP requirements. According to Joint Staff officials, costs for AT/FP continue to rise because new requirements are continually being identified as threat and terrorist tactics change.

According to an Army official, AT/FP requirements are the fastest growing requirement in the Army budget today. He estimated that the Army's AT/FP unfinanced requirement is growing at $80 million per year.[11] Despite this, the Army did not anticipate increasing AT/FP funding for fiscal years 2002

[11]This is an estimate for the Army-wide program, not just the AT/FP programs in Korea, Europe, and the Pacific.

through 2007. According to an Army official responsible for developing the Program Objectives Memorandum, the Army is reluctant to increase spending until it can develop a model that can predict the level of protection obtained for dollars spent. As a result, the Army in Europe has significantly less money than it believes it needs to adequately secure its installations. Specifically, the Army's proposed funding plan for fiscal years 2002 through 2007 underfunds its forces in Europe by $44.2 million in fiscal year 2002 alone, with a total of $226.5 million for fiscal years 2002 through 2007.

The Air Force had anticipated increasing AT/FP spending for fiscal year 2002 when it updated its fiscal year 2002 to 2005 spending proposal this year because requirements were growing as commanders identified vulnerabilities and developed projects to correct them. However, ultimately, the Air Force did not increase funding for its forces in Europe and the Pacific. For fiscal years 2002 through 2007, these forces have unfunded requirements of $37 million and $13 million, respectively.

The Navy hopes to be able to increase AT/FP in its fiscal year 2002 spending plans, but plans beyond fiscal year 2002 are uncertain. A Navy official responsible for making AT/FP funding recommendations for a small portion of the Navy's AT/FP budget told us that he would recommend an increase in some AT/FP spending for fiscal year 2002. The same official told us that it was unlikely that the remaining years of the Program Objectives Memorandum (fiscal years 2003 through fiscal year 2007) would be funded at the fiscal year 2002 level.

DOD Provides Congress With Limited Antiterrorism/Force Protection Funding Information

During consideration of the fiscal year 2000 DOD budget, the Senate Committee on Armed Services expressed concern over its inability to obtain information about DOD's programs to combat terrorism. In its report, the Committee said,

"With current budget submissions, it is difficult for the committee to determine the scale of the Department's effort to combat terrorism, the effectiveness of the effort, how well the Department's efforts respond to the threat, and how the DOD programs fulfill the overall government policy and strategy in this area."[12]

To improve its oversight of combating terrorism activities (which include AT/FP), Congress directed the Secretary of Defense to provide it with a consolidated combating terrorism budget justification (among other things).[13] Congress directed that the consolidated budget justification provide details on how the services intend to spend the combating terrorism funds they are requesting and to provide this information by appropriation as well as by functional areas.[14] Congress did not require DOD to supply any information about unfunded AT/FP projects that would correct or mitigate vulnerabilities. The first consolidated budget justification was submitted in support of the fiscal year 2001 budget request in February 2000.

Program Managers Are Inadequately Trained

Each installation is required to have an AT/FP manager who serves as the "subject matter expert and advisor" to the commander. In general, the AT/FP managers we met were not adequately trained to manage their installations' programs and to complete the tasks assigned by the geographic combatant commanders and services.

DOD has not established specific qualifications for these managers. There are, however, specific tasks that are required of the commanders by DOD directive. Insight can thus be gained into the capabilities required of the AT/FP program managers in support of an installation commander. Based

[12]S.Rept. 106-50, at p. 353 (1999).

[13]National Defense Authorization Act for Fiscal Year 2000, P.L.106-65, section 932 (1999), adding a new section 229 to chapter 9 of title 10, United States Code.

[14]DOD has determined that its AT/FP program consists of seven functional areas: physical security equipment, physical security site improvements, physical security management and planning, security forces/technicians, law enforcement, security and investigative matters, and research, development, test and evaluation.

on these tasks, a manager must be able to adequately plan and exercise an AT/FP program, advise the commander on setting threat conditions, perform physical security vulnerability assessments, coordinate AT/FP response plans for subordinate and tenant organizations on the installation, routinely review the effectiveness of daily security measures, conduct residential security assessments of off-base housing, provide base engineers with military construction requirements, train base personnel, and conduct ongoing awareness programs.

The only formal training DOD offers for these managers, which can be waived by a commander, is designed to teach managers how to provide basic terrorism awareness training to installation personnel. It does not emphasize how to develop or manage an AT/FP program. No formal AT/FP program management training that instructs personnel on how to manage an AT/FP office, garner funding, or that teaches best practices exists. At some installations we visited, the primary method of developing AT/FP expertise was through on-the-job training. As a result, nearly all of the AT/FP managers we interviewed believed they were unprepared to do their jobs:

- Many of the AT/FP managers were not aware of all DOD and geographic combatant command AT/FP requirements. For example, DOD requires that all installations undertake a physical security vulnerability assessment once every 3 years. This requirement was not met at most installations—some AT/FP managers were not familiar with this requirement and others did not know how to conduct a physical security vulnerability assessment.
- Many installations did not have AT/FP plans or had poor ones. These plans are supposed to include procedures to (1) collect and analyze terrorist threat information, threat capabilities, and vulnerabilities to terrorist attacks; (2) enhance AT/FP protection; and (3) respond to terrorism incidents. The plans we reviewed at installations we visited varied in size and scope, from just a few pages to 15 volumes. It was clear that the AT/FP managers had no uniform understanding of what was expected of them in this regard.
- Many installations have never practiced using the AT/FP plans. The plan helps to determine their ability to protect personnel and assets against terrorist attack. If a plan is written, but not workable, it is of little use in an emergency.

- One AT/FP manager we interviewed did not understand the difference between the concepts of THREATCONS and threat levels,[15] despite the fact that his position requires that he act as an advisor to the commander on these topics.

Changes are planned for the AT/FP manager training as a result of a recently completed Joint Staff study of the training. The study found that the current training fulfills current standards but does not teach an AT/FP manager how to be a force protection manager. To make improvements, the Joint Staff (1) reviewed the applicable directive; (2) surveyed the geographic combatant commands, the services, and the defense agencies; and (3) observed current service AT/FP manager training courses. As a result, the Joint Staff drafted a new standard outlining a curriculum that would include training on installation AT/FP manager duties, how to write plans, and how to conduct assessments. While DOD would set the standards for what is taught, each service would still be responsible for independently developing the course of study and completing the training for its own personnel. This could lead to differences in the training from one service to another. For example, one service has already mentioned that it would like to implement a 2-week training course, rather than the current 1-week course. The new standard is currently under review, and it is unclear when it will be implemented.

Conclusions

While all risks cannot be eliminated, they have been reduced through the improvements DOD has made in its ability to protect U.S. forces located outside the United States from terrorist attack. Commanders have used vulnerability assessments to determine the vulnerabilities they face and have developed strategies for correcting those vulnerabilities. The vulnerability assessment reports issued by the Joint Staff do not, however, contain all the information that could be useful to the commander. Also, the Joint Staff has not developed a system to share assessment results, which represents a lost opportunity to learn from the mistakes and lessons of other installations and which could reduce the risks that servicemembers face. As a result of these weaknesses, significant vulnerabilities that place U.S. forces at risk will remain until the services provide the funds and

[15]According to DOD, threat level classification is a set of standardized terms used to quantify the level of terrorism threat on a country-by-country basis. Threat levels are estimates with no direct relationship to specific threat conditions [THREATCONS]. Threat levels should not be confused with threat conditions.

trained personnel that commanders, who are charged with protecting the forces, have determined are needed. Congress does not receive information about the unfunded antiterrorism/force protection projects designed to correct or mitigate vulnerabilities, leaving it unaware of the level of risk that U.S. military members overseas are facing, which limits its ability to provide effective oversight of DOD's efforts and determine appropriate funding levels. Furthermore, while no amount of money or number of personnel can completely eliminate the risk of a terrorist attack, not providing the necessary resources to address identified antiterrorism/force protection program requirements will leave U.S. military personnel unnecessarily vulnerable to terrorist attacks.

Recommendations

To improve the effectiveness and increase the impact of the vulnerability assessments and the vulnerability assessment reports, we recommend that the Secretary of Defense direct the Chairman of the Joint Chiefs of Staff to improve the vulnerability assessment reports provided to installations. Although the Joint Staff is planning to take some action to improve the value of these reports, we believe the vulnerability assessment reports should recommend specific actions to overcome identified vulnerabilities. In addition, the Joint Staff should develop an antiterrorism/force protection best practices or lessons learned program that would share recommendations for both physical and process-oriented improvements. The program would assist installations in finding answers to common problems—particularly those installations that do not receive Joint Staff Integrated Vulnerability Assessment reports or others who have found vulnerabilities through their own vulnerability assessments.

To provide Congress with the most complete information on the risks that U.S. forces overseas are facing from terrorism, we recommend that the Secretary of Defense direct the services to include in their next consolidated combating terrorism budget submission information on the number and types of antiterrorism/force protection projects that have not been addressed by the budget request and the estimated cost to complete these projects. Information on the backlog of projects should be presented by geographic combatant command.

To ensure that antiterrorism/force protection managers have the knowledge and skills needed to develop and implement effective antiterrorism/force protection programs, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to expeditiously implement the Joint Staff's

draft antiterrorism/force protection manager training standard and formulate a timetable for the services to develop and implement a new course that meets the revised standards. Additionally, the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict should review the course content to ensure that the course has consistency of emphasis across the services.

Matter for Congressional Consideration

To improve congressional oversight of the risks that U.S. forces overseas are facing from terrorism, Congress may wish to consider requiring the Department of Defense to provide, as part of its Combating Terrorism Budget Justification documentation, information on the number and type of antiterrorism/force protection projects that have not been addressed by the budget request and the estimated cost to complete these projects. Information on the backlog of projects should be presented by geographic combatant command.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD agreed with two of our recommendations and disagreed with one. The Department's comments are reprinted in appendix II. In addition, the Department also provided technical comments, which we incorporated as appropriate.

Although DOD agreed with our recommendation regarding improvements to the vulnerability assessment reports and the need to develop an AT/FP best practices and lessons learned program, it did not agree to include in its vulnerability assessment reports specific solutions for identified vulnerabilities. As we noted in our report, providing information on solutions would make the reports more useful to AT/FP managers. DOD also stated that it is currently sharing best practices through the Joint Staff's quarterly AT/FP publication and believes that two computer-based systems now in development will also share best practices. While the quarterly newsletter and the computer-based systems are improvements, they are not a best practices program. An effective AT/FP best practices program requires the systematic analysis and cataloguing of problems and proven solutions and thus would be dependent upon DOD's willingness to identify specific fixes to AT/FP problems.

DOD also agreed with our recommendation to improve AT/FP manager training and stated that revised training standards are being coordinated throughout DOD and that the services are revising their courses to meet the

new standards. However, DOD's response did not specifically address a timetable for implementing the training program or indicate that course content would be reviewed for consistency across all the services. Such steps would provide greater assurance that DOD will implement an effective AT/FP manager training program.

DOD disagreed with our recommendation that the services provide Congress with detailed information on unfunded AT/FP projects that would correct or mitigate vulnerabilities. DOD noted that vulnerabilities may be corrected through procedural changes that do not require funding. The Department stated that AT/FP requirements compete against other "critical mission essential" requirements and that it believes that the current planning, programming, and budgeting system is effective. We acknowledged in our report that AT/FP requirements are in competition with other activities. We did not comment on the effectiveness of the planning, programming, and budgeting system except to note that the services had not provided sufficient funds for the AT/FP program in every year since 1996. In addition, AT/FP managers told us that the existing levels of funding limited their ability to address vulnerabilities. Our recommendation that DOD provide Congress with this additional information would not change DOD's current budgeting process. In the past, Congress has required DOD to provide detailed information on unfunded depot maintenance projects and on the backlog of real property maintenance projects to improve its oversight of programs. Since DOD did not agree with our recommendation, we have added a matter for congressional consideration suggesting that Congress require this information.

If you have any questions regarding this letter, please contact me at (202) 512-5140. Key contributors to this assignment are listed in appendix III.

Sincerely yours,

Norman Rabkin
Director, National Security Preparedness Issues

Scope and Methodology

To determine the extent to which the Department of Defense (DOD) has made improvements to its antiterrorism/force protection (AT/FP) program overseas, we visited installations in the European, Pacific, and Central Commands and met with commanders and AT/FP managers and discussed AT/FP improvements as well as problems. We toured the installations to inspect current vulnerabilities and actions taken to correct past vulnerabilities. We also met with AT/FP managers at four geographic combatant commands (European, Central, Pacific, and Southern), U.S. Transportation Command, and the services' major commands to discuss improvements that they had made in their . programs since 1997 and to obtain their views on continuing problems. At the installation and geographic combatant commands and the services' major commands, we reviewed funding documents, AT/FP plans and orders, project lists, minutes of working group meetings, and letters and memorandums documenting command positions on AT/FP. We also reviewed classified Internet resources available from the U.S. Central Command, U.S. European Command, U.S. Southern Command, and the U.S. Army Europe. We interviewed key members of the Joint Staff Directorate for Combating Terrorism, the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict), the Under Secretary of Defense (Comptroller), and the Department of State to obtain information on AT/FP improvements since 1997 and on plans for future improvements. We also obtained their views on problems at the installation, command, and service levels. We reviewed pertinent DOD and service documents, including directives, regulations, and guidance on combating terrorism.

To determine if changes in DOD's process for assessing and reporting vulnerabilities at overseas locations have enhanced the commander's ability to determine the AT/FP vulnerabilities at installations in their area of responsibility, we reviewed and evaluated vulnerability assessments conducted by the Joint staff Integrated Vulnerability Assessment teams and the service teams for the facilities we visited, and discussed the value of vulnerability assessments with installation commanders, AT/FP managers, geographic combatant commanders' AT/FP officers, and AT/FP managers at the services' major commands overseas. We obtained their views on vulnerability assessment problems and potential solutions as well. We also met with the program manager and deputy program manager of the AT/FP program at the Joint Staff Integrated Vulnerability Assessment office to obtain their views on the problems we learned about during our installation visits. Finally, we attended several AT/FP conferences and trainings held by the Joint Staff and the Assistant Secretary of Defense (Special Operations

and Low-Intensity Conflict) to obtain additional information from installation and service AT/FP managers, commanders, and civilian leaders.

To examine the adequacy of AT/FP funding and staff, we interviewed service AT/FP managers and those officials responsible for funding AT/FP from the Departments of the Army, the Air Force, and the Navy and Headquarters, U.S. Marine Corps, to obtain information on prior year funding as well as proposed levels of funding. At each installation and command visited, we met with resource managers or others responsible for determining AT/FP requirements and obtained documents on previous levels of funding and requirements as well as documents that outline future funding requirements and programmed levels of funding. We also reviewed program decision memorandums and program budget decisions relating to AT/FP funding, but we did not attempt to validate the requirements identified by the installations or the commands. We also reviewed Chairman of the Joint Chiefs of Staff's Combating Terrorism Readiness Initiatives Fund submissions for fiscal years 1998, 1999, and 2000 to determine what types of projects were funded by the Joint Staff. We discussed the adequacy of AT/FP training with representatives of the Joint Staff, reviewed the proposed changes to the AT/FP standards for training and discussed training shortcomings with installation AT/FP managers and the AT/FP staff of the geographic combatant commands.

The geographic combatant commands and the component commands we visited or contacted were:

- U.S. Central Command, U.S. Central Command Air Forces, U.S. Naval Forces Central Command, U.S. Army Forces Central Command;
- U.S. European Command, U.S. Army Europe, U.S. Naval Forces Europe, U.S. Air Forces in Europe;
- U.S. Pacific Command, U.S. Pacific Air Forces, Commander in Chief, Pacific Fleet, U.S. Army Pacific, Marine Forces Pacific, U.S. Forces Japan, Commander Naval Forces Japan, U.S. Army Japan, 5th Air Force Japan;
- U.S. Forces Korea, Commander Naval Forces Korea, 8th U.S. Army Korea, 19th Theater Army Area Command, Korea, 7th Air Force Korea; and
- U.S. Southern Command.

The overseas sites we visited, by country, were:

Bahrain

- Naval Support Activity Bahrain

Germany

- Ramstein Air Base
- 104th Area Support Group

Italy

- Aviano Air Base
- 22nd Area Support Group, U.S. Army
- Naval Support Activity Naples

Japan

- Fleet Activity Yokosuka
- Yokota Air Base
- Camp Zama

Korea

- Osan Air Base
- 20th Support Group, U.S. Army
- 34th Support Group, U.S. Army

Kuwait

- Camp Doha, U.S. Army

Saudi Arabia

- Eskan Village
- Office of the Program Manager-Saudi Arabian National Guard Modernization Program
- Prince Sultan Air Base
- U.S. Military Training Mission

Spain

- Naval Support Activity, Rota

Turkey

- Incirlik Air Base

We conducted our review from June 1999 through May 2000 in accordance with generally accepted government auditing standards.

Comments From the Department of Defense

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

SPECIAL OPERATIONS/
LOW-INTENSITY CONFLICT

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

JUN 30 2000

Mr. Norman J. Rabkin
Director, National Security Preparedness Issues
National Security and International Affairs Division
U.S. General Accounting Office
Washington, D.C. 20528

Dear Mr. Rabkin:

This is the Department of Defense (DoD) response to the General Accounting Office (GAO) draft report, dated July 2000, entitled "Combating Terrorism: Action Taken but Considerable Risks Remain for Forces Overseas," (GAO Code 702013), OSD Case 2026. The draft report reflects an expansive research and reporting effort by your analysis team.

The Department concurs with comment on two of the three recommendations in the report, and non-concurs with one. DoD concurs with the need to improve our vulnerability assessment reports and expeditiously implement antiterrorism/force protection manager training standard (Level II). However, DoD non-concurs with including antiterrorism/force protection vulnerabilities into the Department's Combating Terrorism Congressional Justification Book that the Services did not validate or address in their budget requests. The report does not accurately portray the uniqueness and importance of DoD's internal budgeting process in determining resource allocation or validating requirements, nor how commanders are ultimately responsible for determining prioritization of requirements and resources to reduce physical security vulnerabilities.

See comment 1.

Furthermore, the analysis in this report appears flawed with regard to fiscal accuracy and the underlying premise that vulnerabilities are validated requirements. For example, the report states that $52,000 of a $7.9 million requirement was funded, when in fact Service records verified that $7.4 million was indeed funded. There are other errors of this magnitude in the draft report. Additionally, numerous inaccuracies were detected on various charts throughout the report and therefore, do not reflect the Department's strong commitment to combat terrorism. Since it appears the report assumes vulnerabilities are validated requirements, it should not and can not be used as a measure for quantifying DoD's true antiterrorism posture.

See comment 2.

The Department appreciates the opportunity to comment on the draft report as we continue to focus our efforts on the protection of our forces.

See comment 3.

Sincerely,

Brian E. Sheridan

Enclosures:
As Stated

**GENERAL ACCOUNTING OFFICE DRAFT REPORT DATED JUNE 1, 2000
(GAO CODE 702013) OSD CASE 2026**

"COMBATING TERRORISM: ACTION TAKEN BUT CONSIDERABLE RISKS REMAIN FOR FORCES OVERSEAS"

DEPARTMENT OF DEFENSE COMMENTS

RECOMMENDATIONS

RECOMMENDATION 1: Secretary of Defense direct the Chairman of the Joint Chiefs of Staff to improve the vulnerability assessment reports provided to installations. Although the Joint Staff is planning to take some action to improve the value of these reports, we believe the vulnerability assessment reports should recommend specific actions to overcome identified vulnerabilities. In addition, Joint Staff should develop an antiterrorism/force protection best practice or lessons learned program that would share recommendations for both physical and process-oriented improvements. The program would assist installations to find answers to common problems - particularly those installations that do not receive Joint Staff Integrated Vulnerability Assessment reports or others who have found vulnerabilities through their own vulnerability assessments.

DOD RESPONSE:

DoD concurs with comment. The GAO is correct in their analysis that the Joint Staff (along with Defense Threat Reduction Agency (DTRA), the JSIVA executive agent) is taking action to improve the value of Joint Staff Integrated Vulnerability Assessment (JSIVA) reports. The GAO noted in their report (page 14) that the executive summary of future assessment reports would highlight those vulnerabilities that the team believes to be the most pressing. JSIVA reports now include recommendations in the executive summary. Further, the recommendations are broken down into two areas, "Procedural" and "Resources Required." "Procedural" recommendations are those vulnerabilities that the command can address without funding, while "Resources Required" vulnerabilities require the commander to program resources. Entries in both subparagraphs include "actions to overcome identified vulnerabilities."

The GAO also captured the need for the Joint Staff to provide a means for installations to share AT/FP best practices and lessons learned. Several programs to do just this are already in place, or will be shortly. The Joint Staff currently shares lessons learned via quarterly publication of *The Guardian* newsletter. They will further expand a lessons learned program when the web-based JSIVA Information System (JIS-Web) is fielded this summer and when the Joint Vulnerability Assessment Tool (JVAT) comes on line in Feb 2001. DTRA also established and widely publicizes an email account for installations to ask questions and receive best practices, references, expert advice, and lessons learned.

RECOMMENDATION 2: Secretary of Defense direct the Services to include in their next consolidated combating terrorism budget submission information the number of AT/FP vulnerabilities that have not been addressed by the budget request and the estimated cost to correct these vulnerabilities. Information on the backlog of identified vulnerabilities should be presented by geographic combatant command.

DOD RESPONSE:

DoD non-concurs. The analysis in this report assumes that installation vulnerabilities directly translate into validated Service requirement that require manpower or equipment. This is not the case. Vulnerabilities are not requirements that have been validated through the Services' resource process. Additionally, vulnerabilities may be corrected through non-material solutions, such as tactics, techniques, or procedural changes. DoD recognizes that all vulnerabilities can be addressed either programmatically or procedurally, and directs commanders to practice risk management with respect to AT considerations. Moreover, the funding process for AT is not in isolation from other critical mission essential requirements. All requirements compete to ensure the most essential are addressed and funded.

The Department believes the DoD PPBS system is an effective process that reviews CINCs and Services' validated requirements and identifies any shortfalls. Via the Program Decision Memoranda and Program Budget Decisions, the Deputy Secretary of Defense may direct the Services to fund these shortfalls if determined to be of high priority.

RECOMMENDATION 3: Secretary of Defense direct ASD (SO/LIC) to expeditiously implement the Joint Staff's draft AT/FP manager training standard, and formulate a timetable for the Services to develop and implement a new course that meets the revised standards. Additionally, the ASD (SO/LIC) should review the course content to ensure that the course has consistency of emphasis across the Services.

DOD RESPONSE:

DoD concurs with comment. The draft AT/FP manager training standard is contained in a proposed revision to ASD SO/LIC's DoD Instruction 2000.16, "DoD Combating Terrorism Program Standards." DoD Instruction 2000.16 is in coordination throughout the Department. Upon final approval and signature, the CINCS, Services, and DoD Agencies will be obligated to meet the revised training standards set forth. Armed with the knowledge that this change to the DoD 2000.16 is forthcoming, the Services are already engaged in revising their courses and courseware to meet the enhanced standards of the revised DoD Instruction 2000.16.

The following are GAO's comments on the Department of Defense's letter dated June 30, 2000.

GAO Comments

1. We disagree with DOD's implication that the requirements (the funds the installations need to correct or mitigate vulnerabilities) as highlighted in this report have not been validated and therefore should not be reported to Congress. These requirements reflect the judgment of senior flag officers in the Pacific and European commands who are responsible for protecting U.S. forces from terrorist attack and are in the best position to validate requirements. We also disagree that the report does not acknowledge that commanders are ultimately responsible for determining and prioritizing requirements and resources to reduce physical security vulnerabilities. In our report, we clearly state that commanders are responsible for determining what actions to take to correct or mitigate vulnerabilities and that commanders believe that they have not received sufficient funds to correct the vulnerabilities they have determined need attention. Similarly, we have noted that AT/FP needs must compete against other service needs and that this competition begins at the installation level. Additionally, we have, at the request of DOD, included additional information about the Department's budget process to provide a more in-depth picture of the funding process.

2. The dollar figures in our draft report were provided by the service elements of the geographic combatant commands. During a meeting with service representatives to discuss our report, some concerns were raised as to the currency and accuracy of the funding data. While our draft report was at DOD for comment, we again met with service AT/FP staffs and resource managers to discuss the figures and the services provided new data with the necessary documentation. This new data has been incorporated into our report and does not alter our conclusions.

3. We do not assume that all vulnerabilities are validated requirements. This report discusses only those AT/FP requirements that overseas commanders have validated and forwarded to the services for funding.[1] It should be noted that DOD's planned funding for AT/FP projects for fiscal years 2002 to 2007 is $700 million less than required. This level of funding challenges DOD's stated commitment to combating terrorism.

[1]At the suggestion of the Joint Staff, we have clarified this point in our report.

GAO Staff Acknowledgments

Acknowledgments

Raymond Decker, Carole F. Coffey, Jim Reid, and Tracy A. McCaffery Brown made key contributions to this report.

In memory of Donald L. Patton (1942-2000) under whose skilled leadership this review was conducted.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

***Orders by visiting*:**
Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet:
For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- **Web site: http://www.gao.gov/fraudnet/fraudnet.htm**
- **e-mail: fraudnet@gao.gov**
- **1-800-424-5454 (automated answering system)**

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. GI00