The Defense Science Board 1997 Summer Study Task Force

on

DoD RESPONSES TO TRANSNATIONAL THREATS

Volume II
Force Protection Report

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

DTIC QUALITY INSPECTED 2

October 1997

Office of the Under Secretary of Defense
For Acquisition & Technology
Washington, D.C. 20301-3140

19980312 078

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions and recommendations in this report do not necessarily represent the official position of the Department of Defense.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
Oct 97

3. REPORT TYPE AND DATES COVERED
Final 1997

4. TITLE AND SUBTITLE
Defense Science Board Summer Study Task Force on DoD Responses to Transnational Threats, Volume II

5. FUNDING NUMBERS
N/A

6. AUTHOR(S)
Dr. Robert Hermann
Gen Larry Welch, USAF (Ret)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Defense Science Board (DSB)
Office of the Under Secy of Def (A&T)
3140 Defense Pentagon
Washington DC 20301-3140

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
same as above

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
N/A

12a. DISTRIBUTION AVAILABILITY STATEMENT
Distribution Statement A
Approved for Public Release: Distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

14. SUBJECT TERMS
transnational threat
terrorism
WMD
BW/CW
natioanal security
domestic first responders
force protection

15. NUMBER OF PAGES
153

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	N/A	N/A

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

9 Dec 97

Honorable Jacques S. Gansler
Under Secretary of Defense Acquisition and Technology
3010 Defense Pentagon
Washington, DC 20301-3010

Dear Mr. Secretary:

In response to joint tasking from the Under Secretary of Defense for Acquisition and Technology and the Chairman, Joint Chiefs of Staff, the 1997 DSB Summer Study Task Force addressed the Department's Responses to Transnational Threats. In the study, the Task Force concludes that the Department should treat transnational threats as a major Department of Defense mission.

Transnational actors have three advantages: 1) they can have ready access to weapons of mass destruction; 2) we cannot easily deter them because they have no homeland; and 3) they respect no boundaries, whether political, organizational, legal or moral. Further, warning may be short and attribution may be slow or ambiguous. Since the United States is now the dominant military force in the world, potential adversaries will be driven to asymmetric strategies to meet their objectives. As such, transnational threats represent an important national security problem.

Notably, the Department of Defense has the capacity to mitigate these threats with its extensive capabilities, training and experience. In the attached report, the Task Force suggests a multi-faceted strategy for the DoD to address this increasingly important class of threats. This strategy involves the development of an end-to-end systems concept, investment in critical technology areas, and the leveraging of similarities between civil protection and force protection. The Task Force concludes that the Department also needs to increase its emphasis on responding to this threat by more clearly assigning responsibilities and by providing mechanisms for measuring its readiness to respond.

We hope this Summer Study provides insights on how to mitigate transnational threats to the Nation. It stops short, however, of providing a plan. We strongly encourage the Department to take on the task of developing an implementation plan that identifies the appropriate allocation of resources and areas for emphasis.

Craig I Fields
Chairman

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

8 Dec 97

Memorandum for the Chairman, Defense Science Board

Subject: Final Report of the 1997 Defense Science Board Summer Study Task Force on DoD Responses to Transnational Threats

The final report of the 1997 Defense Science Board Summer Study Task Force on DoD Responses to Transnational Threats is attached. This report consists of three volumes: Volume I which presents the major findings and recommendations of the Task Force, Volume II which focuses on force protection and is written expressly for the Chairman, Joint Chiefs of Staff, and Volume III which includes eight supporting reports.

After focusing on this study topic for a period of six months, we concluded that threats posed by transnational forces are an important and under-appreciated element of DoD's core mission. We found a new and ominous trend -- a transnational threat with a proclivity towards much greater levels of violence. Transnational groups now have the means, through access to weapons of mass destruction and other instruments of terror and disruption, and the motives to cause great harm to our society. Since the United States remains the dominant military force in the world now, potential adversaries will be driven to asymmetric strategies in order to meet their objectives.

The Department of Defense has the capacity to mitigate these threats with its extensive capabilities, training and experience. We suggest that the DoD address this increasingly important class of threats through a response strategy that includes six elements:

1. Treat transnational threats as a major DoD mission
2. Use the existing national security structure and processes
3. Define an end-to-end operational concept and system-of-systems structure
4. Provide an interactive global information system on transnational threats
5. Address needs that have long been viewed as "too hard"
6. Leverage worldwide force protection and civil protection

Together these principles will help the Department deal with transnational threats today and in the future. Notably, the task force holds that DoD can respond without a change to national roles and missions, and without change in its own organization. However, the DoD does need to increase its emphasis on this threat, clearly assign responsibilities and measure its readiness to respond. In addition, the

Department should focus more attention on strategies, architectures and plans that address the end-to-end set of capabilities needed.

We thank the Task Force members and the talented group of government advisors for their hard work and valuable insights. Their dedication reflects their belief in the importance of this challenge to the Department.

Robert Hermann, Chairman

Larry Welch, Vice Chairman

TABLE OF CONTENTS

VOLUME II – FORCE PROTECTION

PREFACE iii

EXECUTIVE SUMMARY v

CHAPTER 1: INTRODUCTION 3

CHAPTER 2: PANEL ASSESSMENT 7
- What is Force Protection? 7
- Force Protection Environment 7
- Force Protection Responsibilities 11
- Current Force Protection Activities 12
- Vulnerability Assessments – Lessons Learned 25
- Next Steps 28

CHAPTER 3: ACTIONS REQUIRED 31
- End-to-End Mission Orientation 31
- Expand Vulnerability Assessments 32
- Patch "Seams" Created by Diverse Responsibilities 34
- Exploit Technology 36
- Enhance Intelligence Operations 41

CHAPTER 4: FINAL THOUGHTS 47

ANNEX A. PANEL MEMBERSHIP A-1
ANNEX B. BRIEFINGS AND REFERENCES B-1
ANNEX C. J-34 FORCE PROTECTION PROGRAM C-1
ANNEX D. SERVICE FORCE PROTECTION PROGRAMS D-1

PREFACE

At the request of the Chairman, Joint Chiefs of Staff and the Under Secretary of Defense for Acquisition and Technology, the 1997 Defense Science Board Summer Study task force assessed DoD capabilities, options, and responses to transnational threats. Specifically, the task force was asked to:

- Review the legislation, executive orders, prior studies and current activities of the government,
- Identify the variety of threats which should be addressed by the Department,
- Assess the nation's vulnerability to these threats,
- Examine the DoD capabilities for playing its proper role in response,
- Identify available and potential technologies that may be applicable for enhancing the protection of US Armed Forces, and
- Recommend actions by the Department to position itself properly for this set of problems.

The task force recommends a long-term strategy for DoD's response that leverages the Department's resources and strengths. The six elements of the strategy, discussed in detail in Volume I – Main Report of the 1997 Defense Science Board Summer Study, are:

1. Treat transnational threats as a major DoD mission
2. Use the existing national security structure and processes
3. Define an end-to-end operational concept and system-of-systems structure
4. Provide an interactive global information system on transnational threats
5. Address needs that have long been viewed as "too hard"
6. Leverage worldwide force protection and civil protection

The Chairman of the Joint Chiefs of Staff expressed particular interest in the protection of United States Armed Forces. In response to that request, a Force Protection panel was formed with the specific mission of addressing the Chairman's concerns. This volume addresses the findings and recommendations of the Force Protection panel, which are consistent with and draw on the six elements of the task force strategy.

EXECUTIVE SUMMARY

The 1996 bombing of Khobar Towers in Saudia Arabia refocused the Department's attention on a problem that is not at all new to the military, namely that of force protection. Protecting forces, infrastructure, and lines of communication have long been part of any military mission – whether it be active combat in the Gulf or a peacekeeping mission in Bosnia. Force protection is an enduring command responsibility.

Khobar Towers, like Beirut more than a decade before, had a sobering effect on the US military; the event highlighted the difficulty of protecting forces and the potentially devastating consequences of an attack. To reduce risks, force protection must become a way of life for every member of the US Armed Forces, whether stationed in the United States or abroad. It must become part of the culture or state of mind in every day operations and a central component of mission planning and execution.

What is it that has changed about this mission? Some argue that while the tactics and tools of force protection have changed very little, there has been a significant change in the nature of the threat. Today's forces face a new and more complex threat: the transnational threat. Transnational adversaries appear to be growing more sophisticated and appear to be increasingly interested in inflicting mass casualties and extensive destruction. Further, the inability of these adversaries to threaten the United States with traditional military force drives them to the use of other weapons – high explosives, chemical and biological agents, and potentially even nuclear devices. Moreover, the United States is no longer a sanctuary and is vulnerable on its own soil. This trend has implications both for force protection and protection of civilians at home.

The Chairman of the Joint Chiefs of Staff established a vision for the Department: *to make US forces PREMIER in force protection.* The Force Protection panel supports this vision and believes it is essential for DoD to carry out this vision. A premier force protection capability is not a static condition, but a dynamic one. As such, the Department must put in place the tools and processes to attain and maintain such a capability in a fluid and changing international environment – one dominated by transnational adversaries with methods and motives unlike those faced in the past.

Since Khobar Towers, DoD has taken many steps to improve its force protection posture. While these have been solid efforts, a long-term, sustained campaign plan must be developed and executed to achieve full-dimensional protection for our forces – in or out of combat. The panel believes that an effective, sustained plan must encompass the recommendations summarized below:

- ***Reemphasize force protection as a mission responsibility.*** Force protection must be part of day-to-day operational missions worldwide, not just a wartime

issue. An end-to-end focus should expand force protection to include capabilities for deterrence, detection, and prevention in addition to mitigation and response. The Secretary of Defense should reemphasize force protection as a mission responsibility by elevating its priority in departmental strategy, guidance, and investment and by making force protection a readiness issue. Improving force protection capabilities should also capitalize on the synergy between this DoD mission and civil protection, to the benefit of both.

- ***Expand scope and breadth of vulnerability assessments.*** The vulnerability assessments being conducted by J-34, the Services, and the CINCs provide a useful initiative for evaluating the status of force protection measures throughout DoD. The panel supports the continuation of these assessments but believes that they should be expanded to address a full range of threats. Thus far, the vulnerability assessments have focused primarily on protecting people, but should be expanded to include mission-related targets, essential infrastructure, and lines of communication. The assessments have emphasized ways to mitigate the effects of high explosives, but should be expanded to provide more attention to addressing the chemical, biological, radiological, and even nuclear transnational threats.

- ***Patch the "seams" created by diverse responsibilities.*** Force protection responsibilities span many organizations and offices in the Office of the Secretary of Defense, the Joint Staff, and the Services. The panel is concerned about the many organizational and functional gaps and overlaps that exist as a result of these diverse responsibilities, and their impact in the crucial areas of budget, policy, plans, and programs. The panel recommends that the Secretary of Defense clarify force protection responsibilities within the Office of the Secretary of Defense, that the Chairman do likewise within the Joint Staff, and that the Services review existing assignments of responsibilities.

- ***Exploit promising technologies.*** The Department of Defense should better exploit current and emerging technologies to reduce force protection vulnerabilities. There are a substantial number of technologies that can be employed to enhance force protection capabilities both in the near term using commercial, off-the-shelf products, and in the long term as various new technologies mature. To ensure that the Department exploits these technologies where they add the most value for the dollars invested, the panel recommends the creation of an enduring test bed capability to help facilitate the transition of technology in support of force protection requirements. In addition to the test bed, the panel recommends establishing a five-year technology investment plan for rapid technology insertion.

- ***Enhance intelligence operations for force protection.*** DoD needs to sharply increase its focus on force protection intelligence needs, particularly at the tactical level. Intelligence collection and analysis remain focused on

supporting major theater warfare, but the organization, methodology, and practices that support operational plans do not fully support force protection requirements. There is a need to reorient, improve, and accelerate tactical collection, analysis, and all-source information fusion programs to include coalition partner national assets. Additional human intelligence assets are needed – which are crucial elements in understanding the transnational threat. Intelligence analysts need access to a broader set of national and international data bases. Finally, the panel urges the deployment of tactical intelligence capabilities organic to local units overseas.

These recommendations will, in the Force Protection panel's judgment, go a very long way toward making US force protection capabilities much more robust for dealing with the transnational threat.

CHAPTER 1.

Introduction

"Today, we must concern ourselves with the proliferation of weapons of mass destruction, ethnic discord, inter and intra-state conflicts whose origins have deep historical roots, terrorism and other transnational threats ... ."

CHAIRMAN OF THE JOINT CHIEFS OF STAFF,
GENERAL HENRY H. SHELTON

CHAPTER 1. INTRODUCTION

The transnational threat is a major challenge to the US military and will remain so in the future.[1] US presence, policies and leadership must remain a major stabilizing force in the world, which will require a range of credible offensive military capabilities, forward military presence, surge capabilities, and independent or coalition operations. A credible future global model depicts an environment that will require an activist foreign policy to sustain world stability, continuing foreign presence, and occasional military interventions in areas of conflict. This same model exacerbates stresses that traditionally motivate transnational adversaries. Thus, the transnational threat will become more significant over time.

In response to the Khobar Towers bombing, the Secretary of Defense commissioned the Downing Task Force to assess the facts and circumstances surrounding that tragedy. The findings addressed adequacy of policy, clarity of responsibility, effectiveness of intelligence, adequacy of budget, local national provision of security, use of advanced technology, medical care, adequacy of training, and preparedness of US personnel. Recommendations from the Downing Task Force led to numerous actions within the Department of Defense in all aspects of force protection – in essence becoming a road map for DoD antiterrorism and force protection efforts. The many actions included designating the Chairman of the Joint Chiefs of Staff as the DoD-wide focal point for force protection and issuing a new DoD-wide directive, DoDD 2000.12, *DoD Combating Terrorism Program*, to provide an improved, single standard on force protection. In addition, the Chairman designated a new staff element in the Joint Staff organization, J-34, as the directorate responsible for combating terrorism.

As part of the 1997 Defense Science Board Summer Study, *DoD Responses to Transnational Threats*, the Chairman of the Joint Chiefs of Staff requested that special attention be paid to the subject of force protection. In response to that request, the Force Protection panel was formed with the specific mission of addressing the Chairman's concerns.

The Force Protection Panel, co-chaired by General Al Gray, USMC (Ret.) and Ambassador Henry Cooper, included representatives from the military services, DoD labs, the Joint Staff, the Office of the Secretary of Defense, the Defense Advanced Research Projects Agency, and other force protection experts.[2] The panel focused its efforts on the Department's methods for protecting people and facilities as well as on force protection actions and requirements to combat current, evolving, and future threats. The panel

[1] Transnational threats comprise any transnational activity that threatens the national security of the United States – including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery systems for such weapons, and organized crime – or any individual or group that engages in any such activity. This definition is taken from Public Law 104-293,1996 HR 3259, Section 804.

[2] Annex A contains a list of panel members.

protection and reviewed the findings of the force protection vulnerability assessments currently underway. Of particular emphasis was the examination of how technology can be used to enhance force protection.

In conducting this study, the panel reviewed relevant legislation, executive orders, prior studies, and current force protection activities in the Services and throughout the Department of Defense. The panel received briefings from experts in DoD and private industry. Speakers were drawn from the Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, the Joint Staff's J-34 Directorate, the Defense Intelligence Agency, the National Reconnaissance Agency, the Defense Special Weapons Agency, US Central Command, the Defense Advanced Research Projects Agency, Sandia National Labs, the Army's Waterways Experiment Station, the Office of the Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs, the Office of the Director, Defense Research and Engineering, and each of the military departments.[3]

This report presents the findings and recommendations of the Force Protection panel. To guide its efforts, the panel examined the following characteristics to determine if the United States has an effective force protection program:

- clear policy and goals;
- adequate resources, particularly to address highest priority items;
- operational changes underway and evidence of the ability to evolve with the changing strategic landscape; and
- a mix of procedural and technical solutions at hand to address problems that arise.

While improvements in the Department's force protection capabilities are possible, the panel was mindful of constraints that must be recognized and overcome in order to succeed. They include cultural and institutional bias; civil liberties in both the United States and host countries; the quality of life of US forces which is crucial to an effective fighting capability; political will; and ever present budget constraints. With these factors in mind, the panel has reviewed and appraised the Department's force protection efforts to date and offers recommendations for improving DoD's force protection posture in the future.

[3] A list of briefings presented to the Force Protection panel and other references can be found in Annex B.

CHAPTER 2.

Panel Assessment

"Certainly our level of awareness of the terrorist threat has been heightened .... However, much remains to be accomplished to ensure that our units stationed overseas make this heightened awareness part of their daily routine."

FORMER COMMANDER-IN-CHIEF, US SPECIAL OPERATIONS COMMAND
GENERAL WAYNE A. DOWNING, US ARMY (RETIRED)

CHAPTER 2. PANEL ASSESSMENT

What Is Force Protection?

Force protection, as defined in Joint Publication 1-02, is a DoD security program to protect soldiers, civilian employees, family members, facilities, and equipment, in all locations and situations. Force protection is accomplished through planned and integrated application of combating terrorism, physical security, operations security, and personnel protective services, supported by intelligence, counterintelligence, and other security programs. The publication goes on to describe combating terrorism as DoD actions – including defensive measures to reduce vulnerability to terrorist acts and offensive measures to prevent, deter, and respond to terrorism – to oppose terrorism throughout the entire threat spectrum. These definitions serve as the basis for the panel's analyses – an expansive view of the force protection mission, which includes not only protecting forces but also deterring transnational adversaries and protecting against and mitigating the effects of terrorist acts.

Force Protection Environment

Transnational Threats

As the geopolitical structure of the Cold War collapsed, the environment gave rise to radically new threats to the United States and its interests by organizations and individuals with motives and methods quite different than those posed to the nation during its confrontation with the Soviet Union. These threats, referred to as transnational threats, comprise any transnational activity that threatens the national security of the United States – including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery systems for such weapons, and organized crime – or any individual or group that engages in any such activity.[4]

The motives and methods of the transnational threat are different from those of traditional nation states. The technology of today, and that which is emerging, allows a small number of people to threaten others with consequences heretofore achievable only by nation states. The United States' homeland, allies, and interests are vulnerable. The likelihood and consequences of attacks from transnational threats can be as serious, if not more serious, than those of a major military conflict.

The United States is more vulnerable to transnational threats today than in the past, and this vulnerability is likely to increase. As part of its global superpower position,

[4] This definition of transnational threats is taken from Public Law 104-293, 1996 HR 3259, Section 804.

the United States is called upon frequently to respond to international causes and deploy forces around the world. America's position in the world invites attack simply because of its presence. Historical data show a strong correlation between US involvement in international conflicts and an increase in terrorist attacks against the United States. And, the United States will likely remain a significant target for such attacks in the future.

At the same time, US military operations will be subject to a growing list of vulnerabilities. All phases of combat operations, mobilization, logistics, command and control, engagement, and cleanup will become more dependent on communication and information systems that are susceptible to threat operations. There will be fewer logistic sea and air points of departure and delivery in support of major military operations, which will make departure points more attractive targets for attacks using weapons of mass destruction. Many future operations will be urban operations and require contact with host populations – conditions at odds with today's preferred force protection practices.

Threats posed by transnational forces can interfere with DoD's ability to perform its mission, to protect its forces, and to carry out its responsibilities to protect the civilian population. A robust force protection capability is critical to meet US security needs and maintain the nation's ability to project its forces abroad.

There are many capabilities in the hands of transnational adversaries. While events like Khobar Towers abroad and the World Trade Center bombing at home draw attention to the high explosive threat, the threat from chemical, biological, and other agents have the potential to cause far more devastating consequences.

Chemical and biological warfare agents share characteristics that make them an especially grave threat. They are also relatively easy to obtain, can be developed and produced with modest facilities and equipment, can be extremely lethal even in small quantities, and can be delivered by a variety of means. But chemical and biological materials also have substantial differences. The most important difference, perhaps, is that biological agents can be far more toxic by several orders of magnitude than chemical warfare agents. Thus the range of effects of a few kilograms of chemical agent could extend several city blocks. By contrast, the same amount of a biological agent could threaten an entire city. A second significant difference is that generally the effects of chemical warfare agents occur much more rapidly – minutes to hours versus days for biological agents. These differences must be taken into account when devising strategies and postures to deal with the threat.

The panel urges the Department to be mindful of the threat from nuclear and radiological weapons in planning its force protection program. If the required fissile material is available, it is not difficult to design and build a primitive nuclear explosive device. The diffusion of knowledge and technology over the past decades makes such a task increasingly possible, and a nuclear device could be small and light enough to be transported to an intended detonation point by a variety of means.

Operating at Home and Abroad

Force protection challenges vary significantly between the continental United States and military operations overseas. Force protection overseas can be significantly more difficult in those locations where local communities do not have the infrastructure necessary to support US force protection efforts or where the local communities may not be friendly or cooperative. As shown in the table below, the two most significant differences involve rules of engagement and matters of jurisdiction.

Force Protection Environment

	CONUS	*OCONUS*
Jurisdiction	Better cooperation and concurrent jurisdiction. Have detention authority	None outside fence
ROE	US military can respond to defend personnel or facilities	Very restricted in use of force
Law Enforcement	Cooperative	Less capable May or may not help
Infrastructure	Extensive	Often weak
Threat	Perceived as minimal	Higher level of alert

In the United States, the US military can respond, as necessary, to defend personnel or facilities. Outside national borders, the ability for US military personnel to use force is far more restricted. US forces are heavily dependent abroad on the capabilities of local police or host nation military for security at the point where local jurisdiction is established. Policies for arming deployed US forces varies from country to country, and site to site, and are dependent upon national sovereignty, legal jurisdiction, and policies of the host nation installation commander. In general, US security forces are very limited in their authority to detain suspicious individuals and use deadly force outside of base perimeters.

Generally, US forces have no jurisdiction beyond the perimeter in overseas locations. Also, with few exceptions, the US Chief of Mission, typically the Ambassador, is responsible for the security of Americans who are not under the direct command of the regional combatant commander. Ongoing actions between the Departments of Defense and State seek to establish a formal memorandum of understanding that would permit the regional commander or the Chief of Mission to negotiate which organization can best provide for the force protection of US forces and personnel.

In both the continental United States and abroad, there are common problems created by encroachment of civilian facilities around military installations; the draw-down of US military medical capabilities and what can be considered an over-reliance on civilian mass casualty medical treatment; and the vulnerability and lack of redundancy in supporting infrastructure such as water and electric utilities.

Linking Force Protection to Civil Protection

Another element in the force protection environment is the parallelism between force protection and civil protection. There is a strong synergy between the demands of force projection, force protection, and civil protection, as depicted in Figure 1. A robust force protection capability is critical if we are to meet US security needs and maintain the nation's ability to project its forces abroad. Force protection is part of full-dimensional protection for US forces, extending to family members, civilian employees and facilities, as well as installations, ports, and airfields in both the United States and overseas.

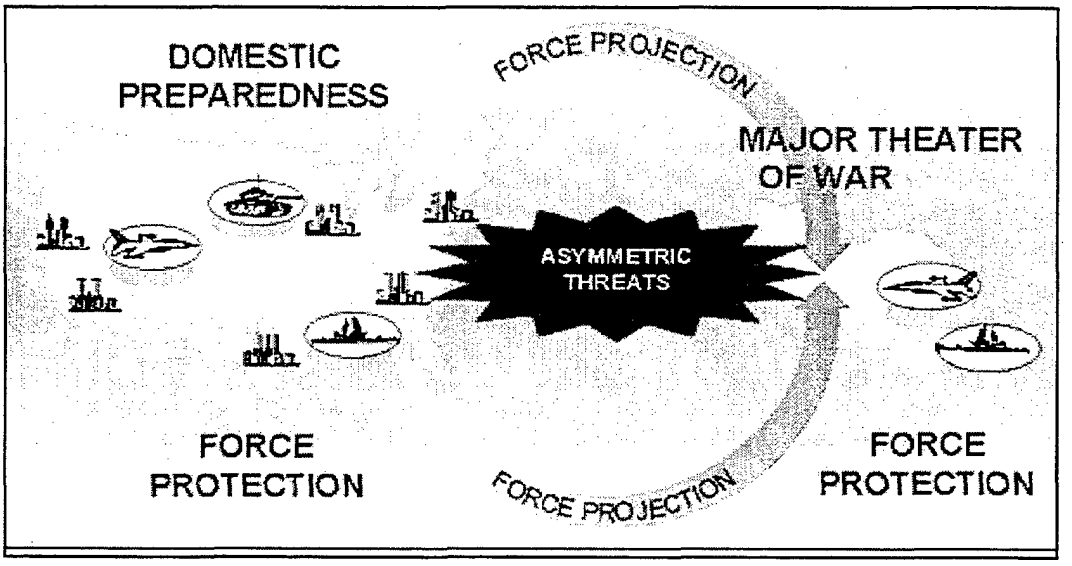


Figure 1. Linkages Between Force Projection, Force Protection, and Civil Protection

When closely examined, the requirements for protecting military facilities against attacks by transnational adversaries have much in common with protecting civilian facilities and people in metropolitan areas. This mission synergy allows the United States to leverage DoD capabilities and expertise for force protection as it may apply to civil protection. There is a vast experience base in the civilian community among first responders – the firefighters, emergency medical personnel, and law enforcement officers who are first on the scene in the event of a crisis. And the existing resources and experience in DoD to cope with the battlefield use of weapons of mass destruction provide another experience base from which to draw. Both the Department of Defense and the civilian community can benefit from this synergism by leveraging capabilities and expertise across both mission requirements.

Force Protection Responsibilities

Force protection is, and always has been, a mission responsibility for the Department of Defense, for its forces at home and abroad. But events abroad, such as the Khobar Towers bombing, have placed renewed attention on this mission. In his September 1996 Report to the President on *The Protection of US Forces Deployed Abroad*, the Secretary of Defense made clear that force protection is a fundamental responsibility of the chain-of-command. Responsibility for force protection rests on the shoulders of each regional and local commander. This responsibility is not new, as force protection has always been the commander's responsibility. What is new is the nature of the transnational threat and how it is dealt with.

The Chairman of the Joint Chiefs of Staff is the "principal advisor [to the Secretary of Defense] and the single DoD-wide focal point for force protection activities." The Chairman is directed to ensure:

- "that our policies will result in adequate force protection measures being taken and for auditing the performance of our units;"
- "that force protection receives a high priority in budgetary allocations;" and
- "a joint and uniform approach to force protection throughout the Service components."[5]

While the Chairman is the focal point, many others have responsibilities for force protection as well. The five regional combatant commanders are assigned special responsibility for ensuring force protection in their areas of responsibility. The Chairman has also indicated to the regional commanders that force protection should be given increased priority. The Services continue to have the primary role to support, acquire, train, and equip their forces to support the force protection mission.

The Secretary also made clear that resource considerations and authority for force protection should be treated as they would be for any other mission objective. Where shortfalls arise, the commanders should raise these deficiencies to the next level of command for resolution.

Underlying this structure is the need for the right "state of mind" at all levels – one that acknowledges force protection as a priority matter and views force protection as part of the objectives of every mission. Such a state of mind becomes the link among related efforts that lead to a premier force protection capability.

---

[5] Secretary of Defense Report to the President, *The Protection of US Forces Deployed Abroad*, September 15, 1996.

Under this new guidance, the J-34 and the military Services have begun to enhance the force protection programs of the Department. The next section describes current and ongoing force protection activities in DoD.

Force Protection Responsibility

- **Fundamental responsibility of chain-of-command**
- **CJCS focal point; responsibilities widespread**
- **State-of-mind at all mission levels**

"Should commanders find they lack the resources or authority necessary to provide force protection, they will raise that deficiency to the next level of command, just as they would should they lack the tools necessary to accomplish any other key mission objective"

SecDef, 15 September 1996

Current Force Protection Activities

As a baseline for evaluating the Department's force protection posture, the Force Protection panel reviewed the activities of the J-34 within the Joint Staff and the force protection programs in each of the four Services.[6] What this review showed is that there is considerable activity ongoing across DoD in the area of force protection. Further, there is considerable commonality of approach among the Services. In a number of cases there is evidence of the revitalization of programs put in place after the 1983 bombing of the Marine Corps barracks in Beirut, Lebanon. *This highlights an important point*: the Services see a need to make force protection inherent in day-to-day operations and that it be taken as seriously as any other mission requirement. A sporadic emphasis on force protection is not prudent.

J-34

The Chairman of the Joint Chiefs of Staff established the Deputy Director for Operations for Combating Terrorism (J-34) in October 1996, as a permanent office within the Joint Staff to deal with all matters concerned with combating terrorism. The mission of the J-34 is to "support the Chairman and the Joint Chiefs of Staff in meeting the Nation's security challenges as they relate to combating terrorism, now and into the next century." Among its responsibilities, the J-34 is to synchronize the military's efforts in

[6] Annex C provides additional information on the activities and organization of the J-34 directorate. Annex D provides further details on the Service force protection programs.

antiterrorism and force protection. To accomplish its mission, the J-34 works closely with each Joint Staff directorate, various intelligence agencies, the State Department, the Federal Bureau of Investigation, and each Service and combatant command.

J-34's initial efforts focused on implementing the 81 recommendations from the Downing Report. The Department has successfully achieved 100 percent implementation of these recommendations.[7] This activity has led to five areas of emphasis for J-34: training, doctrine, and education; resources and technology; operational intelligence fusion; interagency and intra-DoD policy coordination; and standards and assessments. Each area is discussed briefly below.

Training, Doctrine, and Education. The J-34 has launched a four-tier training initiative and a multi-level education program that includes training for the individual, unit, commander, and senior executive. Level I provides training to each individual and family member to increase their personal protective awareness. This level involves general training as well as area-specific briefings prior to deployment. Level II training is designed for the unit antiterrorism or force protection officers who will act as the commander's subject matter experts and will be trained to provide Level I training to the unit. Level III training is designed to inform commanders of their responsibilities under current DoD policies, and Level IV is an executive level seminar conducted several times per year in conjunction with the National Defense University.

Other initiatives are planned and will incorporate antiterrorism and force protection training into the basic and officer-level schools and senior-level colleges, so that every member of the armed forces receives both initial and sustainment training throughout their careers. The goal of these programs is to encourage service personnel to incorporate antiterrorism and force protection into their mindset so that these issues are considered in all aspects of military operations, exercises, and daily operations worldwide.

The J-34, working with the Operational Plans and Interoperability Directorate (J-7) and the Joint Warfighting Center, is currently publishing a revised Joint Pub 3-07.2 "Joint Tactics, Techniques and Procedures for Antiterrorism." This document, revised in the wake of Khobar Towers and other terrorism incidents, sets forth the tactics and procedures governing the joint conduct of US antiterrorism operations.

Resources and Technology. The J-34, in cooperation with the Office of the Secretary of Defense, is working on initiatives to heighten awareness of technology applications and provide a process for field commanders to solicit solutions for high-priority, immediate force protection needs. The J-34 manages the Combating Terrorism Readiness Initiative Fund, which provided $24 million to the combatant commands in fiscal year 1997 to fund emergency or other unanticipated force protection requirements that arise from changes in the threat level, political situation, or force protection doctrine

[7] All but two recommendations were implemented: one action was rejected by the Secretary of Defense and one was redirected by the Chairman.

or standards.[8] Currently, $15 million is available for fiscal year 1998 requests. The J-34 is also involved in processing Service requests to the DoD Physical Security Equipment Action Group and the Interagency Technical Support Working Group. The J-34 is responsible for the DoD Force Protection and Physical Security Equipment Technology Guide and has hosted a Force Protection Equipment Demonstration to familiarize commanders and decision makers with available technology.

Operational and Intelligence Fusion. The J-34 Operations and Intelligence Division is engaged in working actions at all levels with both the operational and intelligence communities. All sources of intelligence and operational requirements are evaluated to ensure all necessary force protection measures are being addressed. The development of a "premier" force in combating terrorism and institutionalizing force protection for the security and safety of US forces is the paramount objective of these tasks.

The Operations and Intelligence Division provides the catalyst for interaction with other elements of the Joint Staff (J2 and J3) on antiterrorism and force protection issues. That fusion process, along with coordination from the Defense Intelligence Agency (DIA), results in operational and intelligence information to enhance force awareness and readiness.

J-34 continually monitors DIA's worldwide Threat Levels, geographic combatant commanders Threat Conditions, and applies the all source intelligence and force structure requirements to ensure the best possible force protection antiterrorism posture is achieved. The J-34 also maintains close coordination with the combatant commanders and the Service force protection offices to ensure that concerns from these organizations are addressed and to keep them apprised of the latest threat warning information.

Policy Coordination and Planning. J-34 provides the primary policy interface with the Office of the Secretary of Defense, the combatant commanders, the Services, and DoD agencies for all antiterrorism and force protection matters. This involves coordinating various policy documents, both within DoD and other executive branch organizations. In addition J-34 is developing a Combating Terrorism Plan that will provide operational planning, guidance, and directions to institutionalize the requirements, training, standards, resources, and behavior needed to safeguard US forces from transnational threats.

Standards and Assessments. The J-34 supports drafting, publishing, and updating standards and policies at the OSD and Joint Staff level. In July 1997, a new DoD Instruction 2000.16, *DoD Combating Terrorism Program Standards*, was signed that includes DoD-wide standards for combating terrorism. This instruction contains 33 standards that provide the Department with a common, but flexible, force protection

[8] CJCS Instruction 5261.01, *Combating Terrorism Readiness Initiative Fund*, establishes policy and procedures to facilitate execution of the fund.

foundation and provides guidance for developing Service and agency-level standards, requirements for training, and plans for collecting and analyzing threat information.

Perhaps the most visible of the J-34 activities are the vulnerability assessments, which play a key role in the force protection programs for all commanders. This new assessment program was initiated in fiscal year 1997. It is complemented by assessments performed by the individual Services and the nine combatant commanders. The J-34, in close cooperation with the Defense Special Weapons Agency, the executive agent, has recently formed five Joint Staff Integrated Vulnerability Assessment teams that will visit more than 566 facilities and installations. Fifty assessments were scheduled through December 97, with plans to increase to 100 assessments annually in subsequent years.

The Joint Staff assessment teams provide independent vulnerability assessments to assist commanders in meeting their force protection responsibilities. Over five days, the teams review site features, plans, programs, and procedures and assess tactical warning actions, physical security systems, guard force procedures, incident response, and consequence management capabilities. The teams provide local commanders observations and recommendations for improving their force protection programs as well as information on the types of force protection capabilities available to address their shortfalls. In parallel, the Services have a wide-ranging series of initiatives underway to address force protection. General trends from these assessments are discussed at the end of this chapter.

DoD/CJCS Force Protection Focus

Initial efforts have been on:

- **Force protection standards**
- **Vulnerability assessments**
- **Executive-level training**
- **Policy development**
- **Service and CINC program and budget review**
- **CINC / JROC requirements integration**
- **CJCS Initiative Fund in support of force protection requirements**

High Marks for Initial Efforts, But Concerned About Where to Go From Here

Army

Force protection incorporates active and passive measures taken to preserve the combat power of the force. It is the application of organizational, material, and procedural solutions to the challenges of protecting personnel, information, and critical resources across the full spectrum of operational environments. The US Army force protection program is based upon multi-layered offensive and defensive capabilities designed to ensure full-dimensional protection of our forces both in garrison, as well as during deployment, maneuver, and engagement. Commanders will develop comprehensive force protection programs utilizing select measures which include, but are not limited to, safety, preventive medicine, anti-mine, anti-fratricide, and Antiterrorism Force Protection, which the commander orchestrates to manage risk.

Antiterrorism Force Protection is the security portion of force protection. This program synchronizes select security programs into comprehensive defensive measures to protect our personnel, information, and critical resources against threat attacks. Antiterrorism Force Protection targets the foreign and domestic terrorist threat, as well as those criminals, violent protesters, saboteurs, and foreign intelligence agents that support terrorism, promote conditions beneficial to the conduct of terrorist operations, or otherwise conduct operations to further agendas at the expense of the US Army and its missions. The Army's program is coordinated and integrated with host nation (civil and military authorities overseas), allied forces in combined operations, federal, state, and local law enforcement communities and is incorporated in plans and operational orders.

Since the Khobar Towers bombing on June 25, 1996, the Army has initiated or expanded the emphasis on several programs to ensure the continued protection of soldiers, Department of the Army civilians, and family members from terrorist attack. The Army staff and key functional major commands continue to aggressively work the policy, doctrine, training and education, intelligence, funding, and operational aspects of the Army Antiterrorism Force Protection program. Components of the program and major actions are highlighted below.

Policy. The current baseline policy for the Army Antiterrorism Force Protection program is contained in AR 525-13, the Army Combating Terrorism Program. The regulation has been rewritten by the policy proponent, Antiterrorism and Force Protection Branch, and is expected to be published during the first quarter of fiscal year 1998. The new regulation, titled Antiterrorism Force Protection (AT/FP), will implement mandatory DoD antiterrorism force protection standards, as well as recommendations from the Headquarters Army Force Protection Assistance Team. DoD has staffed and published 33 performance-oriented standards which the Army has embedded, with Army-unique requirements, into 32 Army Antiterrorism Force Protection Standards that will be published with the new regulation.

Doctrine. TRADOC (Combined Arms Command), with assistance from Headquarters Army, is working on development of Army Antiterrorism Force Protection

doctrine. The foundation for this doctrine was originally included in FM 100-37, Countering Terrorism, which has been rescinded. In order to embed Antiterrorism Force Protection throughout the Army's warfighting doctrine, Headquarters Army and TRADOC are working closely to incorporate Antiterrorism Force Protection doctrine into the Army's core warfighting manuals (FM 100-5, FM 100-15, FM 100-20, FM 100-40, and FM 71-100).

Training. The Army leadership is actively involved in ensuring that Antiterrorism Force Protection training is embedded within all levels of command and the professional military educational system. Although the Army already has 15 training courses to support force protection, this program is being revised to align it more closely with current force protection policy, and to capitalize on specific lessons learned. The Army has also implemented the four-level DoD training program, described previously. The Army is developing a simulation package to use in training programs and at local installations as a tool to exercise installation antiterrorism plans, crisis management teams, and response forces. There are also plans to require an annual comprehensive force protection exercise that will evaluate the entire response system in the Army, from threat conditions, to attack warning systems, to consequence management plans. The goal of all training initiatives is to instill force protection as an element of command discipline from planning through execution.

Intelligence. Intelligence is another area in which considerable effort is being focused. A primary goal is to improve intelligence products for commanders, with emphasis on disseminating international terrorist information obtained through a wide variety of sources. There are ongoing funding initiatives to enhance counterintelligence reporting from the field, to train intelligence analysts in counterintelligence for force protection, and to add additional personnel to increase analysis in the force protection area. In addition, there is an Army Reserve Augmentation initiative underway to increase analytical resources in the Army Counterintelligence Center.

Funding. The Army has identified over $1.1 billion in annual programming for force protection-related activities. The force protection mission is embedded in almost every Army activity, but the core of these resources is devoted to physical security equipment, program management, guard forces, law enforcement, antiterrorism, installation counterintelligence, and protective service program elements.

Assessments. Of note in the Army's program is the Force Protection Assistance Team. This team was chartered to provide an overall assessment of the Army's force protection capabilities and identify requirements unique to the Army. The team conducted a series of 16 visits during the first half of calendar year 1997 to select installations, and the assessment results have been briefed throughout the Army. Although the Force Protection Assistance Team completed its charter in July 1997, this effort continued with major command assessments of subordinate commands and installations, Department of the Army Inspector General oversight of major command programs, and the Joint Staff Integrated Vulnerability Assessments (JSIVA) of Army

installations. During calendar year 1997, five Joint Staff assessments were completed in support of Army major commands. Twento-two Army JSIVAs are scheduled for calendar year 1998. Additionally Army Regulation 525-13 requires that the Antiterrorism Force Protection programs in all Army installations be reviewed by the major commands and all commanders will review the Antiterrorism Force Protection programs of their lower echelon/subordinate units every three years.

Technology. The Army's Physical Security Equipment Program is a key component of its overall force protection program. It is through this program that the Army is bringing the latest technology into the field to counter the threat. The Army was also the lead Service involved in publishing the DoD Physical Security and Force Protection Guide, which will serve to educate commanders at all levels on available technology to support force protection requirements. The Army was a lead player in the successful commercial off-the-shelf force protection equipment demonstration at Quantico, Virginia, in September 1997. Additionally, the Army is leveraging technology in areas beyond physical security equipment. The Army considers information operations to be a major pillar in the design of its force protection program. Antiterrorism force protection is a key consideration in the development and application of technology in the Army's supporting Command and Control Protect Program.

Information Integration. The Army has taken steps to integrate its many force protection initiatives through a steering committee and information dissemination efforts. The Force Protection Steering Committee Board of Directors was established to help ensure that requirements are identified, tracked, and completed. The board includes representatives from the key functional staff elements and commands responsible for oversight of the Army force protection program. Also, the combatant commands have developed home pages identifying critical force protection issues in their area of responsibility. These pages, along with others that contain information on force protection issues, historical data, current threat information, and links to related force protection sites, are available online throughout the Army community via secure intranets. The Army's annual Worldwide Antiterrorism Conference serves as a continuing forum to exchange ideas and to generate policy recommendations related to force protection. The 1997 Conference, with the theme "Antiterrorism Force Protection in the New Millennium," focused on the nature of the terrorism threat in the future and current force protection efforts.

The Army has identified five challenges that must be overcome to maintain a fully effective force protection program. They are: ensuring force protection standards are implemented, providing resources to meet critical force protection requirements, disseminating information on terrorist threats facing the Army, focusing training on the current threat, and sustaining a changed mindset. Overcoming these challenges will be the focus of continuing force protection efforts.

Navy

The Navy's antiterrorism and force protection program is implemented with direction from the Chief of Naval Operations' (CNO) staff. The N3/N5 antiterrorism/force protection cell, working in concert with the Naval Criminal Investigative Service (NCIS), is the Navy's single point of contact for force protection matters to:

- provide unity of effort between the Navy, Joint Staff, and combatant commands;
- provide a uniform approach to DoD standards, education, and training;
- implement an assessment program that provides assistance to installation commanders; and
- prepare, through the vulnerability assessment process, for the next level of terrorism, to include chemical, biological, nuclear, and information warfare attacks.

The Chief of Naval Operations has reemphasized an existing program, resulting in early successes in antiterrorism and force protection program implementation.

Training. The Navy has implemented a four-level training program. Level I is directed at individual and personal protection awareness. From there, Level II training addresses unit force protection, Level III involves leadership training, and Level IV provides senior executive courses. The comprehensive nature of this program is specifically designed to ensure that every person throughout the chain of command understands force protection as part of their individual responsibilities.

All levels of training are underway. In the first year since implementation, over 500 force protection officers and 2,100 antiterrorism training officers have completed Level II training; and over 300 executive and commanding officers have completed Level III training. The Navy has also implemented a pre-deployment antiterrorism and force protection certification process for all units deploying overseas. Unit commanders must certify that antiterrorism awareness training is complete prior to deployment and that their unit security and force protection plans take antiterrorism considerations into account.

Policy and Funding. The Navy has been involved in the DoD force protection policy review process. As instructions are released by the Secretary of Defense, Department of Navy instructions are released down to the unit level. The Navy has also taken steps to ensure greater visibility into force protection funding, with reporting requirements that highlight areas for physical security equipment, site improvements, and management, security forces, law enforcement, security investigations, and research and development. The current Navy budget for antiterrorism and force protection is approximately $3 billion over the future years defense plan (fiscal years 2000-2005), with about 90 percent for manpower costs and the remainder for funding day-to-day

operations, procurement, and research and development. Future focus of the Navy's budget will be on employing new and commercial off-the-shelf technologies to enhance security including screening devices, security force equipment, electronic security systems, communications equipment, and deployable security teams and equipment suites.

Technology. The Navy labs are working on numerous force protection research and development efforts. Examples of recent efforts include: swimmer detection sonar to assist in waterside security; shipboard physical security program which involves research in biometrics; digital recording; portable explosive detection; entry point screening; and infrastructure hardening techniques such as glazing and blast mitigation efforts.

Vulnerability Assessments. The Navy's integrated vulnerability assessments are linked to DoD standards and are scheduled in coordination with the Joint Staff vulnerability assessments. The purpose of the program is to evaluate antiterrorism and force protection vulnerability and make recommendations to improve the force protection posture at an installation. Up to 40 assessments are being conducted per year, in an effort to cover 124 Navy installations in a 3-year period. In fiscal year 1997, 17 Navy assessments and 10 Joint Staff assessments were completed. In fiscal year 1998, 20 Navy and 17 Joint Staff assessments are scheduled, with a shift to combining Navy and Joint Staff teams to provide a regional assessment of Navy concentration areas or regions, such as Norfolk and San Diego. The assessment team provides reports to the facility commanders for action. The Navy is analyzing the results of these assessments to identify emerging trends, which become the basis for inputs to the programming and budgeting process, developing force protection strategy and guidance, and training.

All installations are required to conduct an antiterrorism and force protection self assessment. While ships are not part of the installation vulnerability assessment schedule, an assessment approach has been developed which combines top down inspections with bottom up unit pre-deployment assessments.

The Navy agrees that the challenges to successful long-term implementation are significant. To change the mindset and ensure that antiterrorism and force protection is institutionalized in naval operations means that perceptions toward force protection must change. The message to the Navy's personnel is that force protection is a long-term program and it is the job of every member of the force.

Air Force

In November 1996, the Chief of Staff of the Air Force directed the Service to restructure the Air Staff to provide a focal point for force protection. He also set in place a number of objectives for the Air Force force protection program that encompassed coordination with other organizations, force awareness, intelligence, information dissemination, and technology applications. Key organizations involved in Air Force

force protection are the Air Force Security Forces Center, the 820th Security Forces Group, and the Force Protection Battle Lab.

The Air Force Security Forces Center (HQ AFSFC) was established at Lackland Air Force Base, Texas in November 1997, combining the staffs from the Air Force Policy Agency at Kirtland AFB, New Mexico and other staff members from the Pentagon. The Air Staff Force Protection Division (HQ AFSFC/SFP) was initially established at the Pentagon in January 1997, to provide force protection resource advocacy, policy, and guidance to the field. This new division, led by an O-6 under the Director, Air Force Security Forces Center, is a multidisciplinary organization composed of Security Forces, Office of Special Investigations, and exchange officers from the US Army and the Royal Air Force Regiment. The division relocated to the Security Forces Center in August, 1997.

In addition to the new Air Force Security Center, two other organizations were also established at Lackland AFB, Texas. The 820th Security Forces Group is a cohesive, multidisciplined force capable of rapid deployment and ready to employ measures necessary to ensure optimum protection of Air Force resources and personnel. The group is involved in training in a wide variety of areas to include base defense, intelligence, chemical and biological warfare, air assault, regional orientation, terrorism, and post-blast analysis. The force is equipped with sensors and surveillance systems, thermal imagers, body armor, communications, and other technology. The group stood-up in March, 1997 and reached full operational capability in October 1997.

The Force Protection Battle Lab is focused on exploring and integrating technology, tactics, and training to increase force protection readiness. This organization, one of six Air Force Battle Labs, is a multdisciplinary unit manned by representatives from the Security Forces, Office of Special Investigations, Intelligence, Civil Engineering, Explosive Ordnance Disposal, Communications and other specialties, as required. Areas where the Force Protection Battle Lab focuses its efforts include exploiting existing/conceptual technology, optimizing tactical sensor systems, developing innovative application of commercial-off-the-shelf systems, exploring ways to complement military working dog capability with emerging explosive detection technology, integrating chemical/biological detection systems, and applying UAV potential to force protection. The organization stood-up in April 1997 and reached full operational capability in October 1997.

The Air Force program encompasses six areas: operations, personnel, physical security, equipment, intelligence, and training.

Operations. The Air Force has issued new force protection guidance, AFI 31-210, *The Air Force Antiterrorism Program.* The Air Force is also developing its own vulnerability assessment concept of operations based on the Joint Service Integrated Vulnerability Assessment model. The Air Force Office of Special Ivestigations Antiterrorism Specialty Team conducts vulnerability surveys, countersurveillance, and

high-risk protective service operations; deploys with the Security Forces Group, establishes source networks, and collects intelligence on the terrorist threat. These six-person teams are a repository of force protection expertise and function as a rapid response force protection capability. In the Southwest Asian area of operations, the Office of Special Investigations has also increased surveillance operations, protective services operations, and protection measures for convoy routes. Both the Security Forces Group and Air Force Office of Special Investigations Antiterrorism Specialty Team have demonstrated their capabilities in deployments supporting force protection operations.

Personnel. In the US Central Command area of responsibility, the Air Force has more than doubled its security forces theater wide and has identified increases for intelligence and special investigations. There has also been a move to extend rotations from 90 to 179 days for 18 special investigators and the Joint Intelligence Chief to improve continuity within the theater. Several critical force protection positions in Southwest Asia were converted to one-year assignments to provide long-term continuity in key leadership positions.

Physical Security. In the area of physical security, the Air Force has relocated forces in Saudi Arabia from dense urban areas to less vulnerable locations. This effort also included widening perimeters; improving surveillance and detection; construction of more robust protective measures such as fences, barricades, and berms; hardened entry control points and barriers; and modular facilities. A $48 million integrated electronic detection and assessment system has been installed around the bases in Southwest Asia and buys for other locations worldwide continue.

Equipment. The Air Force has accelerated the deployment of equipment including hand-held thermal imagers, low-light video systems, mini-intrusion detection systems, night vision devices, remote viewing kits for thermal imagers, and under-vehicle surveillance systems. Funding has also been accelerated for the Tactical Automated Security System, a deployable perimeter intrusion detection system. The Air Force has added $162 million in fiscal years 1998-2003 to the force protection spending initiatives worldwide.

Intelligence. The Joint Task Force commander in Southwest Asia created the Force Protection Fusion Cell at Eskan Village. This cell gathers and processes all-source data and provides theater-specific analysis. This ensures timely, analyzed information is provided to wing commanders and is shared with security forces and the Office of Special Investigations. Intelligence personnel will augment deploying security force units to serve as direct liaison for intelligence information. The Air Force is working actively with the Director, Central Intelligence, to create guidelines for sanitization and release of intelligence information. The Defense Intelligence Agency has extended the Defense Intelligence Threat Data System to the Air Force and Navy counterintelligence organizations.

Training. The Air Force has also implemented the four-level force protection training program to provide force protection training at all levels on a recurring basis. Annual training conducted by the Office of Special Investigations and other specially trained members is provided to all Air Force personnel at home station and prior to all deployments. Installation antiterrorism/force protection points of contact receive specialized training in a program administered by the Air Combat Command. Pre-command courses also present antiterrorism/force protection blocks of training. Senior leaders attend seminars at the National Defense University. Additional training initiatives are being developed for all levels of accession training, professional military eduation, and other areas where antiterrorism/force protection is appropriate.

The Air Force is addressing force protection issues across a wide front. Deployed forces are better protected and less vulnerable, and improvements will continue. The Air Force is reorganizing to maintain proper institutional focus on force protection. Resource concerns are identified and receiving higher priority. As in the other Services, an important element of the Air Force program is changing the "culture" to embrace force protection requirements. The Air Force is active in all DoD efforts to protect personnel. Overall, the program being put in place will help ensure that the Air Force can anticipate and protect against an ever-changing threat.

Marine Corps

Force Protection is an overarching concept. It includes those procedural, training, equipment, and leadership principles necessary to ensure the safety and well-being of Marines, their family members, and civilian employees. Marine Corps force protection has its foundation in two basic tenants that have endured throughout the Corps' history: first, Marines take care of their own; and second, commanders are ultimately responsible for the security of their personnel. To this end, the goal is to focus on those areas that can best be influenced, such as training and education, proper operational planning, and providing the necessary resources to ensure the highest level of protection for Marine personnel.

Doctrine and Regulatory Guidance. Five key documents provide guidance for the Marine Corps Force Protection Program.

- Combating Terrorism is formally addressed within doctrinal publication Fleet Marine Force Manual (FMFM 7-14, *Combating Terrorism*). Additionally, Fleet Marine Force Reference Publication (FMFRP 7-14A, the *Individual's Guide for Understanding and Surviving Terrorism*) provides individual awareness information. Both documents will be introduced into the Marine Corps Doctrinal Publication series in the next revision.

- The Marine Corps policy regarding Combating Terrorism is formally set in Marine Corps Order 3302.1B. The Order is currently under revision and will incorporate both US Marine Corps prescriptive and DoD performance-based standards addressed in DoD Instruction 2000.16.

- Specific policy regarding physical security measures for Marine Corps activities is set forth in both OPNAVINST 5530.14B, *Department of the Navy Physical Security and Loss Prevention Manual* and OPNAVINST 5530.13B, *Physical Security of Conventional Arms, Ammunition and Explosives*. This instruction establishes uniform security standards for US Navy and Marine Corps activities. Its next revision will incorporate the 33 standards identified by DoD and the J-34 in DoD Instruction 2000-16.

In addition to the above documents, the Marine Corps Force Protection Campaign Plan is currently being staffed. Once approved, this document will clarify the issue of force protection and provide commanders with a source document for institutionalizing local programs.

Training and Education. Marine Corps Order 3302.1B requires the designation of unit antiterrorism officers at the battalion/squadron level and higher to effect a viable antiterrorism program. A key part of this program is the requirement that all personnel receive annual terrorism awareness training. Enlisted Marines in the pay grades of E-1 through E-7 are tested annually on antiterrorism as part of the Marine Corps' Essential Subjects Testing Program. Additionally, Marines may enroll in a correspondence course through the Marine Corps Institute entitled "Terrorism Awareness."

To assist commanders in the conduct of their combating terrorism program, the Marine Corps has instituted specialized training for selected categories of personnel. This training includes the US Army's Antiterrorism Instructor Qualification Course and the Individual Terrorism Awareness Course at Fort Bragg, NC; the US Army's Combating Terrorism Abroad Military Installations Course and Conventional Physical Security Course at Fort McClellan, AL; and the US Air Force's Dynamics of International Terrorism Course at Hurlburt Field, FL.

MCO 3302.1B also specifies that terrorism scenarios be incorporated into field training and exercises. Additionally, each Marine installation is required to conduct an annual terrorism exercise in order to evaluate the installation's ability to counter or contain a terrorist threat. This requirement was recently reemphasized in All Marine (ALMAR) message 333/96. The Marine Corps has also implemented training to meet the Chairman of the Joint Chiefs of Staff requirement to provide force protection and antiterrorism training to all deploying personnel within six months of deployment.

Vulnerability Assessments. The Marine Corps currently conducts assessments with the goal of looking at force protection vulnerabilities "from both sides of the fence." The assessments are conducted using a "systems approach" that covers such areas as physical security, access control, threat warnings and indicators, and exercises and emergency reaction plans. This methodology provides a comprehensive look at the physical security of facilities, operating procedures, adequacy of resources, and the ability to implement measures for higher threat conditions. All Marine Corps installation assessments are coordinated with the J-34.

Security Enhancements and Initiatives. The Marine Corps maintains a dedicated and centrally managed physical security program which aids commanders in meeting security requirements. Current funding for fiscal years 1998 and 1999 is approximately $5.4 and $5.8 million respectively, increasing to $9.0 million annually for fiscal years 2000-2003. Enhancements identified in fiscal years 2000-2003 include funding for two civilian analysts at Marine Corps Headquarters, assessments of installation and operating forces, mobile training teams, and electronic security system upgrades. The Marine Corps will continue to embrace technology where feasible in meeting future force protection requirements..

The Marine Corps is participating in various DoD and Joint Staff forums which serve to enhance force protection efforts, to include the Joint Warfighting Capability Assessment on combating terrorism, Antiterrorism Coordinating Committee and Senior Steering Group, Physical Security Equipment Action Group, the Joint Security Chiefs Council, and the Physical Security Review Board. In September 1996, the Headquarters Marine Corps Force Protection Working Group was formed to address antiterrorism/force protection related issues.

The Marine Corps established the Chemical-Biological Incident Response Force (CBIRF) that provides an impressive capability to respond to chemical and biological terrorist threats. The Corps also maintains other dedicated security assets to enhance force protection capabilities to include Military Police – Installation Special Reaction Teams, military working dogs trained in explosive detection, dedicated organic counterintelligence and human intelligence capabilities, and the Marine Corps Security Force Battalion – Fleet Antiterrorism Security Teams.

While none of these actions can guarantee that Marine personnel will never again be the target of transnational threats, they aid in reducing the opportunity for transnational adversaries to focus their attack on Marine personnel. The Marine Corps is keenly aware that the security of personnel and equipment is an inherent function of command. Force protection will remain an integral part of the way we do business on a daily basis.

Vulnerability Assessments – Lessons Learned

In addition to conducting the joint vulnerability assessments, the J-34 reviews each assessment report for common trends among commands and identifies lessons learned and observations. The J-34 is very proactive in providing this information to local commanders. This information is made available, via a secure DoD web page, to commanders in the field to assist them in improving the force protection programs in their own installations.[9] The findings from these initial assessments, summarized in the

[9] Information from the vulnerability assessments is provided to field commanders via the Global Command and Control System, a classified DoD network. Access is available to the combatant commanders, the Services, and appropriate DoD offices.

chart on page 27, served as a starting point for the panel's review of the Department's force protection activities.

Initial assessments by the Joint Staff teams and by the Services and combatant commanders are generally consistent in their findings. Perhaps most notable is that despite efforts to elevate the importance of force protection, the transnational threat does not receive priority attention in many locations. There is a certain apathy – or ambivalence – perhaps because commanders believe force protection investments may come at the expense of mission, morale, welfare, and quality of life. Operations and maintenance budgets, where force protection investments are generally addressed, are already squeezed, even before considering investments to mitigate transnational threats.

Deficiencies exist in training and equipping security personnel. Policies governing assignments in overseas installations vary, with an impact on training, readiness, and situational awareness. In some cases, short duration tours preclude development of host nation counterpart relationships or situational awareness at the deployed location. Moreover, insufficient assignment lead time can preclude unique training for the area of operations prior to deployment. Continuity is important in these overseas situations and often was found to be less than desired. Also, because of increased operational and personnel tempo, installations are experiencing a reduction of security and law enforcement personnel despite increased requirements.

Physical security and standoff distance for blast protection are common problems. In addition, in many posts overseas, US personnel are heavily reliant on host nation, third country, and contract labor for physical security services which can raise unique security concerns. Moreover, overseas rules of engagement can be very restrictive, limiting US pre-emption and response options – policies vary from country to country, and are dependent on national sovereignty, legal jurisdiction, and host nation rules and preferences.

Notable shortfalls exist in capabilities for chemical and biological attack detection, characterization, warning, and mitigation. Most of today's capabilities to respond to chemical and biological agents are terrain oriented, based on battlefield requirements related to a major theater war. While substantial transfer exists, the transnational threat is more likely to be characterized by events involving facilities or installations, and is more likely to occur in urban or heavily populated areas. There is a need for much more emphasis on detailed planning and technological solutions for mitigating the threat from weapons of mass destruction. Installations lack detailed plans for responding to these incidents, and units lack detection capabilities and personal protective gear.

US forces are particularly vulnerable while deploying to theaters of operation, while moving in groups within the theater, and while conducting routine day-to-day business. Overseas billeting and operational facilities are generally small, are

inadequately designed to protect inhabitants from modern weapons, and are not necessarily collocated, requiring the use of vulnerable modes of ground transportation.

The vulnerability assessments to date have pointed to the need for local, organic, tactical intelligence collection and fusion capabilities that bring together information specifically relevant to addressing unique force protection challenges in specific locations. Some installations lack formal plans with local police forces and Federal Bureau of Investigation field offices for threat assessments and tactical warning.

The assessments have also identified a trend among commanders which indicates a lack of up-to-date knowledge about potential technology solutions for antiterrorism and force protection programs.

While the vulnerability assessments are progressing and problems are being identified, the panel observed that the progress in fixing problems seems slow. This may appear to be the case because there is no agreed way to measure the benefits of ad hoc recommended solutions and the competition for dollars. Overall, the Force Protection panel believes that reducing force protection vulnerabilities requires a combination of procedural and technological enhancements.

Vulnerability Assessments Findings

- **Some apathy remains**
- **Risk mitigation measures may come at the expense of mission or morale, welfare and recreation**
- **Security personnel not fully trained and equipped**
- **Physical security and blast standoff generally deficient**
- **Chem and bio detection, characterization, warning, and mitigation are deficient**
- **Personnel vulnerable in transit**
- **OCONUS rules of engagement too restrictive**
- **Heavily reliant on host nation, third country, or contract labor**
- **Limited tactical intelligence collection and fusion capability**

Reducing Vulnerability Requires Procedural and Technological Enhancements

Next Steps

Force protection is a major responsibility for the Department of Defense, for its forces at home and abroad. The Department has taken steps to improve its force protection programs as the new threat emerged. The prior discussion summarizes major actions and programs under way. In general, DoD deserves high marks for these efforts, but the panel concluded that much more remains to be done. The findings of the initial vulnerability assessments point to areas where substantial effort is needed.

The panel has targeted five areas where further progress can be made by DoD. An enhanced force protection program needs: an end-to-end mission orientation, expanded vulnerability assessments, patching of "seams" created by diverse responsibilities, exploitation of promising technologies, and an expanded focus on tactical intelligence programs and organic intelligence capabilities.

CHAPTER 3.

Actions Required

"Force Protection is the most difficult near-term challenge we face as an Army."

CHIEF OF STAFF OF THE ARMY
GENERAL DENNIS J. REIMER

CHAPTER 3. ACTIONS REQUIRED

The panel identified five key areas where enhancements to the Department's force protection measures should focus. This chapter discusses each area in more detail. An important criteria for fulfilling these actions is that force protection become a "state-of-mind" throughout DoD and a constant way of life, based on a common understanding among all US forces. It is this focus on "state of mind" that is necessary for DoD's force protection efforts to be truly effective.

End-to-End Mission Orientation

Force protection must be part of day-to-day operational missions, not just a wartime issue. Specialized units – such as special forces, DELTA force, Navy Seals, Strategic Air Command, and many Marine Corps units – take this approach all the time. These units focus every minute of every day on the commander's intent: it is part of their culture. Force protection must be explicitly dealt with at all levels of the chain-of-command involved in executing the mission, including infrastructure and the lines of communication – airfields, ports, and mission-critical lodgments enroute. Incorporating force protection scenarios in war games and exercises can help to sustain, and even raise, the level of awareness and emphasis on force protection.

An end-to-end focus gives a broader view to the force protection challenge. It includes capabilities for detection and proactive prevention as well as deterrence, mitigation, and response. Although not the focus of this panel's efforts, a broad perspective also recognizes the synergy between the demands of force protection and civil protection, and the necessary integration with the civilian crisis response community and other civil/military requirements.[10] The Force Protection panel urges that the force protection mission focus on the fullest range of plausible threats including chemical, biological, nuclear, and radiological warfare as well as high explosive and information operations threats.[11]

The Secretary of Defense should reemphasize force protection as a mission responsibility by elevating its priority in departmental strategy, guidance, and investment.

---

[10] The synergy between force protection and civil protection is discussed in further detail, including additional recommendations, in Volume I – Main Report of the Defense Science Board 1997 Summary Study Task Force on DoD Responses to Transnational Threats.

[11] Though not a focus of the task force, information warfare is an important component of the transnational threat and the force protection challenge. Volumes I and III of the Summer Study report contain further discussion of this topic as does the recently published report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* and the 1996 Defense Science Board Study, *Information Warfare-Defense.*

This orientation is consistent with the overall Defense Science Board Summer Study Task Force recommendation for a comprehensive end-to-end operational architecture to focus the varied and diverse elements throughout the Department of Defense and to prepare a cohesive, strategic response to the transnational threat.[12] Within that context, a similar focus on force protection is called for. This is the right perspective from which to identify technology needs and requirements; identify priorities for research, development and acquisition; and conduct exercises, training, and red teaming that respond to the force protection challenge.

Total Problem -- End-to-End Mission

- **Make force protection part of Commander's intent and a "state-of-mind" -- today it is NOT**
- **Interrelate with civil response / civil-military requirements**
- **Include detection, deterrence, proactive prevention**
- **Prepare for chemical, biological, radiological warfare as well as high explosive threats**

Integrate Force Protection with Operational Mission

Expand Vulnerability Assessments

The vulnerability assessments conducted by J-34 provide a useful initiative for evaluating the status of force protection measures throughout the Services. ***The panel supports the continuation of these assessments but believes that they should be expanded to better address the broader transnational threat.***

Thus far, the vulnerability assessments have focused primarily on protecting people, as have many of the current Service force protection programs. The panel urges that the assessments be expanded to include mission-related targets, essential infrastructure, and lines of communication in an end-to-end mission context – bridging operations in both the United States and overseas. At a minimum this would include critical infrastructure associated with the rapid deployment and reinforcement of US forces, communications, and transportation networks. Within the continental United

[12] Volume I contains a detailed description of this important recommendation in Chapter 2.

States, where assessments have focused more on procedures and less on physical security or infrastructure, a more expansive perspective must be taken.

Further, the assessments have also emphasized what can be done to mitigate the effects of high explosives. This should be expanded to provide more attention to chemical, biological, radiological, and even nuclear transnational threats. The assessments should also address a broader application of technical solutions to mitigate force protection vulnerabilities, beyond the low-cost or commercial-off-the-shelf technologies to which the recommendations tend to be limited.

The Joint Staff vulnerability assessment process has been designed to complement the range of inspections and assessments being conducted by the separate Services and the Unified Commanders. The intent, in selecting the Defense Special Weapons Agency to provide an assessment capability for the Joint Staff, was not to create additional problems for field commanders. Thus the assessment process was designed not to be inspection oriented in order to avoid the adversarial relationship that can develop with an inspection process. *On the other hand, the Services and the CINCs reported to the panel that they strongly favored making the assessments more inspection-like so that appropriate follow-up action and attention would result.*

The panel agreed with this later view and believes that the assessments should become more prescriptive and inspection-like, with compliance monitoring throughout the chain of command. This would include steps such as adding quantitative objectives and thresholds for improvements. Also, force protection scenarios should be added to the inspection regimes so that commanders and their installations focus on the transnational threat and potential responses. The US Central Command has initiated an inspection-oriented assessment program that could serve as a useful model. Further, the panel recommends that force protection be made a key element of the Service readiness programs to ensure that the interest and attention on force protection does not wane.

Expand Vulnerability Assessments

- **Include mission and infrastructure as well as people**
- **Expand to include chemical, biological, and radiological considerations in all assessments**
- **Strengthen assessments through inspection and compliance monitoring**

Incorporate in All Service Readiness Programs

Patch "Seams" Created by Diverse Responsibilities

The Force Protection panel is concerned about the many organizational and functional gaps and overlaps that exist for force protection in the crucial areas of budget, policy, plans, and programs. These "seams" proliferate across many DoD organizations and offices with various responsibilities. The J-34 has a substantial job managing force protection policy issues throughout the DoD bureaucracy, as well as the interagency community. Force protection interests and programs exist in many offices throughout the Office of the Secretary of Defense. Today, the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict has policy, program, and budget oversight for counterterrorism, antiterrorism, and force protection and is the focal point for DoD's interagency activities. The Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs (ATSD[NCB]) has responsibility for counterproliferation and issues concerning chemical and biological agents, and many of these efforts have force protection implications. Within the Office of the Undersecretary of Defense for Policy lies responsibility for infrastructure protection. And the Office of the Director for Defense Research and Engineering has oversight for all science and technology planning, programming, and budgeting efforts – many related to force protection.

The military Services also have force protection responsibilities. The military police or security office in each Service has functional responsibility for force protection. The Services create force protection requirements and maintain and execute force protection budgets. Potentially problematic seams existed within the Joint Staff – with the J-33 maintaining responsibility for counterterrorism and with the J-34 focusing on antiterrorism and force protection. And the interagency environment, essential to DoD's overall force protection activities, is even more complex with a multitude of seams. At a minimum, the National Security Council, Departments of State and Energy, the Federal Emergency Management Agency, and the Federal Bureau of Investigation are involved at various times, as are numerous state and local government organizations.

The diverse responsibilities for force protection cause friction and militate against unity of effort. No single organization has total oversight of the DoD force protection program. No single organization can account for the overall force protection budget. And no single organization can develop a complete list of today's force protection activities, identify shortfalls, or prioritize the things that should be done to resolve shortfalls.

Force protection acquisition programs are highly fragmented and the relationship between these activities and force protection policies or recommendations from vulnerability assessments is weak. Requirements tend to be the responsibility of facility commanders without any overall integration or synthesis. There is also no focal point for overall system design, engineering, and integration functions. This makes it difficult to

develop a coherent, end-to-end approach to force protection that results in harmonized plans and policies. Without a coherent program, issues and requirements can fall through the organizational seams. Incorporating force protection into a system-of-systems architecture should help to ensure integrated policies and plans and to provide a mechanism and process for generating joint requirements and shared solutions.

The panel recommends that the Secretary of Defense clarify force protection responsibilities within the Office of the Secretary of Defense and that the Chairman do likewise within the Joint Staff. Moreover, the Secretary should elevate the priority of force protection policy by ensuring that the departmental guidance and vision statements emphasize and support force protection as a major DoD mission.

While force protection has received increased visibility in the wake of Khobar Towers, the panel is concerned that this emphasis will decline and complacency will set in – as is the tendency over time. Along with this renewed priority must come a strengthening and streamlining of the requirements process in support of force protection initiatives. Today, it is extremely difficult to sort out force protection activities from most other activities in the budget, particularly for operations and maintenance funded efforts. Responsibility for the force protection budget is spread across many organizations. The Assistant Secretary of Defense for Special Operations and Low Intensity Conflict oversees engineering and technology development for counterterrorism and antiterrorism capabilities on behalf of the military Services. The ATSD(NCB) manages development of counterproliferation capabilities as well as chemical and biological defense. The military Services do not have their own separate research and development or procurement accounts for force protection initiatives.

To some extent this situation occurs because force protection is so closely integrated with many other mission responsibilities. But the Department should have an investment strategy that identifies and prioritizes both near-term and long-term requirements for force protection. This strategy should include requirements for training, equipment, and technology investment. The Services would then execute their force protection responsibilities within this overall architecture.

Recent Progress. The panel is pleased to report that since the Defense Science Board task force deliberations, which concluded in August 1997, steps are being taken to streamline force protection responsibilities. Effective November 24, 1997, J-34 will incorporate the Special Operations Division (J-33/SOD), which brings together the planning and responsibility for antiterrorism, counterterrorism, and force protection into J-34. The new organization will be called the Deputy Directorate for Combating Terrorism/Special Operations (J-34). J-34 will be the Joint Staff focal point for the Office of the Secretary of Defense, combatant commands, Service headquarters, and interagency coordination on all terrorism issues.

Likewise, the Secretary of Defense, in his *Defense Reform Initiative Report*, proposes organizational changes in the Office of the Secretary of Defense that will help to

consolidate force protection responsibilities. Patching the seams that exist cannot be done overnight. These steps within the Joint Staff and the Office of the Secretary of Defense represent an important start in the process.

Patch "Seams"

Diverse Responsibilities for Force Protection Cause Friction and Militate Against Unity of Effort

- Clarify force protection responsibilities within OSD
- Elevate priority of force protection policy
- Ensure defense guidance and vision support force protection
- Strengthen and streamline requirements process
- Create an investment strategy

Demand Synergism At All Levels

Exploit Technology

The Department should further exploit current and emerging technologies to reduce force protection vulnerabilities and to detect and deter attacks.[13] There have been a few technology development programs related directly to force protection. The Defense Special Weapons Agency and the Army Corps of Engineers are developing technologies related to hardening against blast effects and modeling and simulation of blast and other hazardous agent effects. Modest programs drawing primarily on off-the-shelf technology are being applied to some elements of the force protection problem through the Joint Physical Security Equipment Program. Efforts within this program include detection systems, advanced sensors, electronic security system test and integration, and advanced entry control systems.

The Technical Support Working Group (TSWG) is an interagency group that conducts research, development, and prototyping of counterterrorism technologies, and provides a forum to discuss ongoing executive branch antiterrorism and counterterrorism research and development to address near-tern unsatisfied operational requirements. The focus is on hardware for limited use systems and prototypes for operational use. Example projects include on-site vulnerability models, a national data base of all foreign and

[13] The Science and Technology chapter in Volume III contains an extended discussion of technology options with application to force protection.

domestic military and commercial explosives, a mechanical car bomb extractor, and a remote nuclear detection system. The Services should take more advantage of these mechanisms for technology insertion. The J-34 is trying to increase interest in these opportunities.

The Force Protection panel believes that the lack of any substantial technology program for force protection is a symptom of the fragmented ownership of the force protection issue. Without a unifying element to manage force protection requirements and assure that gaps and duplication of effort are purposeful, rather than accidental, a coherent technology program is unlikely. There is a need to create a better mechanism for the operational users in the field to influence science and technology efforts to mitigate force protection vulnerabilities. Moreover, the panel has observed an overall reluctance to seeking technological solutions to force protection shortfalls. Instead, improvements thus far appear to center more on procedural changes or are limited to helpful, but insufficient commercial off-the-shelf technology. This is appropriate for immediate improvements, but over the long term, initial efforts should be extended to include mature and emerging technologies using an integrated systems approach.

The panel concluded that there are a substantial number of technologies that can be employed to enhance force protection capabilities both in the near-term using commercial, off-the-shelf products, and in the long-term as various new technologies mature. These technologies should be evaluated and integrated into an enduring force protection test bed, discussed below.

The areas listed in the chart which follows show where technology might be helpful. In the left column are functional needs that are fairly independent of transnational threat scenarios. The right column lists a substantial spectrum of technologies that the panel believes should be investigated to improve our overall force protection posture in the near term. The list is not intended to be exhaustive – but to indicate that there are many good ideas, many of which are not being leveraged. In the past, force protection has not been among the focus areas for either the Director, Defense Research and Engineering, or the Director, Defense Advanced Research Projects Agency, but will be a focus area for fiscal year 1998. While there are no silver bullets, primary technologies are emerging in these areas:

- all-source information/intelligence fusion at the local, tactical level,
- low-cost blast mitigation techniques which could be retrofitted into facilities,
- real-time characterization of multiple chemical and biological agents using tactical detector systems,
- high-powered microwaves to neutralize some biological and chemical weapon threat options,
- novel decontamination means,
- multi-sensor area and entry point screening; waterside and shipboard physical security systems,

- rapid cargo inspection systems, and
- rapidly deployed barriers and force protection equipment suites.

The issue for the Department is how to exploit such possibilities to assure they add the most value for the dollars invested – a careful analysis of vulnerabilities and the abilities of various technologies to deal with them must be made.

Force Protection Technologies: Some Options

Needs	*Enabling Technologies*
Enhanced Perimeter Security Detect/Assess Delay Entry Control	Rapidly Deployable Systems for Perimeter Protection Automated CCTV Monitor Vehicle Explosive Detection Vehicle Tags/Tracking Deployable Barrriers
Extend Perimeter More Standoff - Area Surveillance	Thermal Imager Wide Area Surveillance Covert Ground-Based Sensors UAV Sensors Microrobotics for Surveillance
Protection Enroute (air, land, sea)	Missile Defensive Warning Active Missile Countermeasures
Intelligence, Indications and Warning	Force Protection Fusion Terminal BW/CW Sensors
Neutralization of Threats	BW/CW Countermeasures UV Disintegrator of Biowarfare Agents
Reduction of Consequences	Construction/Glass Hardening Shock Attenuators
Enhanced Exercises/Training	Quantitative Assessment Methodology Realistic Exercises Real Time Gaming

In the Fall of 1996, the J-34 held an industry day – an opportunity for industry to share with DoD technologies and products germane to the force protection task. A similar event was held in September 1997 at the Marine Corps Base Quantico, Virginia. These events have served to showcase potential off-the-shelf technologies, which exist in abundant quantity. There are many options for improved sensors, perimeter barriers, blast protection, and other enhancements in force protection. But these events leave the selection and integration processes to the local commanders. And evaluation of the best options among the wide range of choices for a particular operating environment is a daunting technical and operational challenge. Force protection is so broad that it demands an integrated approach be taken to applying technological solutions to operational problems.

Currently there is no screening process available to help the local commander determine what technologies or products would most effectively meet his needs. What is needed is a reduction-to-practice process where various piece-part suggestions and demonstrations can be integrated into a more comprehensive approach to increasing force protection in an overall, end-to-end mission context. Moreover this integration must be accomplished within the context of operations plans and constructed to deal with realistic

threat scenarios. That the integration process must take into account very specific threat and operating environments suggests the consideration of a "virtual" test bed, rather than a single location or testing facility. With one organization overseeing and coordinating such a "virtual" test bed, the individual Services could conduct tests oriented to very specific requirements, but that might be of benefit to many users.

The panel recommends the creation of a virtual test bed to help facilitate the transition of technology in support of force protection requirements. The development of a force protection test bed that involves the users in the evaluation process would have the added benefit of sustaining the necessary focus on force protection as a continuing effort. The test bed should be an integral part of the 18-month architecture study recommended by the Task Force.[14] The panel recommends that the force protection test bed initiative be assigned to the Joint Forces Command, as proposed in the Report of the National Defense Panel, or should DoD not establish this organization, to the Atlantic Command. The Joint Forces Command is to be a common force provider to all other commands and would be responsible for directing joint battle laboratories and for conducting and overseeing joint experimentation and innovation efforts, and would be responsible for all joint modeling, simulation, analysis, and concept development – all assets and responsibilities that would position the command to effectively involve the users and technologists in the test bed activities. The test bed initiative should be funded with an initial investment of about $10 million per year beginning in fiscal year 1999.

Force Protection Test Bed

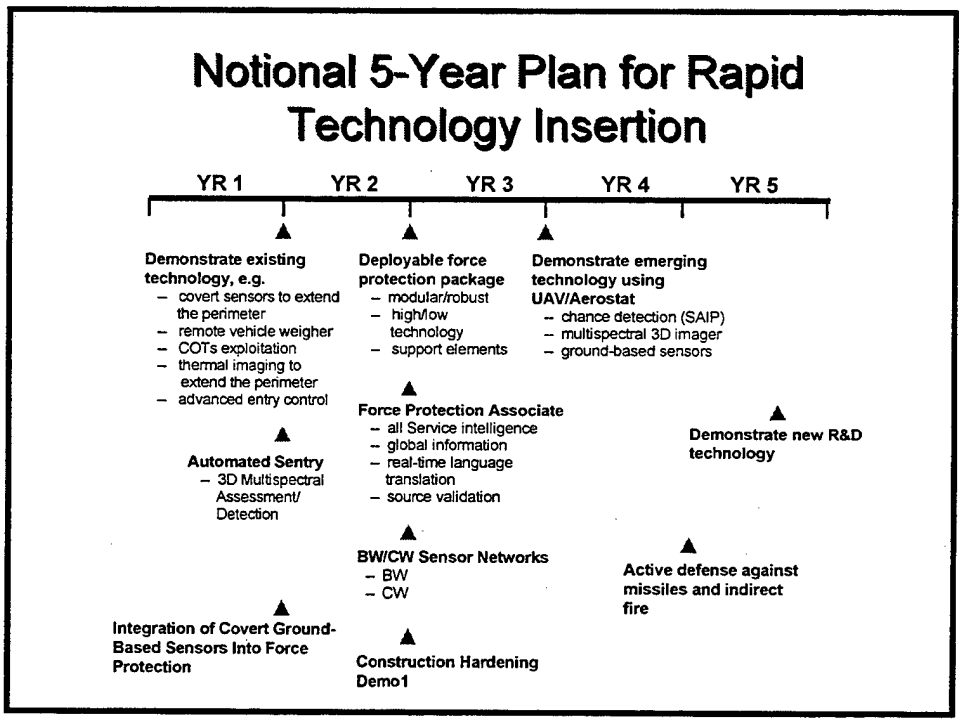
- **Objectives**
  - Evaluate and select technology in an integrated system concept
  - Involve users in requirement and operational system tradeoffs
  - Use "red team" techniques
  - Minimize cost/time to get enhancements to the field
  - Ensure seams are addressed
  - Sustain force protection as a continuing effort
  - Leverage current and prior related programs
- **Management**
  - Joint Forces Command or USCINCACOM
- **Initial Funding**
  - Recommend reprogramming $10 million in FY98 to begin
- **Accomplish in concert with proposed JCS/USD(A&T) architecture study**

In addition to the test bed, the panel recommends the development of a five-year technology investment plan. The first year of a notional plan would focus on

[14] Specifics on this task force recommendation can be found in Chapter 2 of Volume I.

demonstrating off-the-shelf technologies and on moving important improvements to the field quickly. The following figure provides suggestions of what might be accomplished in later years, as a first iteration. The transnational threat architecture should incorporate such a plan for technology insertion and have a major impact on the specifics of this particular plan.

While the details of this chart are not its focus, the main message is that a well-thought-out plan, integrating new technology with existing capabilities, is essential to rapidly fulfilling force protection requirements. The plan also provides a structure within which to evaluate the costs and benefits of applying various technologies to specific force protection problems. As the plan matures, it could be possible to create deployable force protection augmentation packages with new technologies, to be used by field commanders, that are tailored to a specific area of operation and set of threat conditions. These packages would include tools such as ground-based sensors, unmanned and manned aircraft sensors, barrier and area denial means, anti-vehicular means, facility hardening and protection systems, and personnel protective gear. Moreover, such a plan can incorporate requirements and technology demonstrations for equipment that can be used by consequence management teams for both civil and military applications.



One promising new technology that is part of the five-year plan, is the force protection "associate" – a collection of integrated software tools that local commanders can use to perform facility vulnerability analysis, such as determining blast effects on a specific building, and risk management modeling, such as portal and road vulnerability analysis and evaluation of the vulnerability of individual structures. The force protection

"associate" could also include a wide range of other tools such as intelligence data harmonization and fusion, information on transnational threat organizations, local activity monitoring, potential activities and plans of transnational adversaries, and information sharing.

Many of the pieces of the force protection associate have been developed or are currently being studied for their applicability in other military environments. The task at hand is to integrate them into a useful product focused on force protection. The payoff from such an endeavor is a software tool that can correlate information on vulnerabilities with information on potential plans of transnational adversaries. Decision aids such as this would allow site commanders to identify and prepare for countering hostile transnational threat activities. The development of the force protection associate is being evaluated by the Defense Advanced Research Projects Agency.

Enhance Intelligence Operations

Effective intelligence indications and warning are an essential part of any force protection architecture, but intelligence capabilities and efforts are not yet sufficiently focused on this problem. Intelligence gathering and analysis has become highly tailored to the needs of the combatant commanders in support of major regional contingencies. This same level of attention must be devoted to the transnational threat in general, and force protection requirements in particular, consistent with the recommendation in Volume I to "treat countering transnational threats with the same emphasis as major military conflicts." ***DoD needs to sharply increase its focus on force protection intelligence and information needs because they are different than preparing for a major regional conflict.***

Intelligence collection and analysis remains focused on supporting major theater warfare. Intelligence analysts organic to deployed units are trained and proficient in enemy order of battle as described in operational plans. But, they are not as well trained in the tactics and techniques of transnational adversaries or the methods of collecting and analyzing information on the transnational threat, and this needs to be corrected. The intelligence organization, methodology, and practice that supports operational plans is not sufficiently suitable to supporting force protection requirements.

There is a need to develop a new approach – to assess capabilities and limitations of existing collection systems and information fusion techniques; to develop mission-unique capabilities for understanding the transnational threat; to develop improved capabilities for indications and warnings; and to develop the capabilities to identify and understand motivations, track individuals and groups associated with the activities of transnational adversaries, and, in general, create a transnational threat data base that is much better than what exists today. This is consistent with the task force recommendation for a Secure Transnational Threat Information Infrastructure – a two-

way global information system that would expand the available sources of information on the transnational threat. This information system would support gathering more data from the bottom-up, exploit international information sources, and facilitate the sharing and analysis of information collected by different organizations. The result would mean global distributed data bases, held at numerous security levels, and accessible by a global information sharing community.[15]

There are many restrictions on US human intelligence and counterintelligence collection operations in overseas locations. In many cases US forces are not authorized by the host nation to conduct counterintelligence activities outside the facilities they occupy. Overall, the development of all-source, integrated collection and assessment capabilities and the ability to provide intelligence that is targeted to unit requirements in the field are still not mature. The additional step of focusing these resources on force protection is also only just beginning.

Improvements in classified intelligence and open source information require enhancements to both collection and processing. It is important to note that steps to enhance intelligence operations require a coalition approach. Including coalition partners will add to the available data and improve the analysis of transnational threat activities.

In the collection area, there is a need to reorient, improve, and accelerate collection at the local level as well as collection at the global level using the Global Information Infrastructure and the World Wide Web. Intelligence collection on transnational threats must balance its focus among threats from explosives and nuclear, chemical, and biological agents. Further, additional human intelligence and counterintelligence assets, trained for combating transnational threats and equipped with appropriate tools, are needed. Human intelligence and signals intelligence are crucial capabilities in understanding intentions and plans of transnational adversaries, and perhaps the only means to collect meaningful tactical intelligence about the chem/bio threat. Technological innovations in language processing, miniature reporting systems, and communications show promise.

In the processing area, added focus on timely warning and plausible threat identification is essential. Today's trend analysis is weak and often misleading. Analysts tend to accumulate data on transnational threat activity against US interests. Acts against non-US targets are not accounted for, yet these events may be the best forecast of future attacks on the United States. Thus, information that can be important to understanding the future threat may not be incorporated into long-range threat analysis. There is a need to increase the amount of training for analysts to improve predictive analysis, level of detail, and long-term analysis.

National terrorism data bases are not integrated sufficiently to support sharing and fusing of relevant information. Intelligence analysts need access to a broader set of

[15] Volume I contains an expanded discussion of the Secure Transnational Threat Information Infrastructure and the Global Information Infrastructure.

national and international data bases including law enforcement and commercial data bases, such as those contained in the proposed Secure Transnational Threat Information Infrastructure discussed in Volume I. The panel also urges the availability of tactical intelligence capabilities organic to local units. The ability to fuse intelligence data at the local level, and to capture the information crucial to the mission and activities of the local commander is essential.

In addition to improving intelligence operations to better support the requirements for force protection, it is essential that the Department stop the erosion of intelligence resources. The need for human intelligence and special signal intelligence operations to collect information on transnational adversaries is not consistent with a draw down of intelligence assets. Nor is the need to develop appropriate tools to enhance the ability of the intelligence community to respond to the transnational threat. Thus, there is still a need for increased intelligence capabilities that are focused on the future threat environment.

Enhance Intelligence Operations

Focus more on timely warning, deterrence, and prevention. We must:

- **Sharply increase focus on force protection intelligence needs -- *they are different!***
- **Reorient, improve, and accelerate tactical collection, analysis, and all source fusion programs**
- **Upgrade covert capabilities and tools**
- **Increase HUMINT and counterintelligence allocation trained to combat transnational threats and especially include coalition partner nations**
- **Broaden access to national and international data bases including law enforcement and commercial**
- **Stop erosion of intelligence resources -- reallocate and refocus**
- **Ensure availability of tactical intelligence capabilities**

Use Intelligence to "Extend the Perimeter"

CHAPTER 4.

Final Thoughts

"The overall goal ... is to make sure that ... we make American forces the preeminent force in force protection so that the day will come ... where people will come to us and say how in the world do you do this?"

FORMER CHAIRMAN OF THE JOINT CHIEFS OF STAFF
GENERAL JOHN M. SHALIKASHVILI, USA (RET.)

CHAPTER 4. FINAL THOUGHTS

Historically, the Department's emphasis on force protection has been prompted largely by major events such as the bombings of the Beirut barracks and Khobar Towers. Certainly within the past 18 months, the Khobar Towers bombing led to the initiation of many force protection activities and refocused others within the Department of Defense, and these have been solid efforts. But after the urgency of "major events" subsides, often the momentum for addressing solutions slows as well. With regard to force protection, this was observed to some extent in the years following Beirut. Today's challenge is to maintain focus on force protection even in long stretches of time without attacks. Indeed, as force protection measures become even more effective, these times will grow longer in duration. Discipline and tenacity will become critical elements of success.

The transnational threat will continue to be part of the security environment facing the United States into the next century. Responding to this threat requires long-term emphasis. The Chairman of the Joint Chiefs of Staff established a vision to make *US Forces PREMIER in force protection.* The panel supports this vision and believes it is an essential goal for the Department. As such, ***a long-term, sustained campaign plan must be developed and executed to achieve full-dimensional protection for our forces -- in or out of combat.*** The panel believes that, to be effective, a sustained plan must encompass the recommendations summarized below.

Recommendations for Force Protection

- Emphasize Force Protection as a mission responsibility
- Expand scope and breadth of vulnerability assessments
- Demand synergy among policy, plans, and programs; create investment strategy
- Frame a 5-year technology plan around architecture study and integrated technology test bed
- Enhance intelligence operations for Force Protection

Go Operational -- Force Protection is a "State-of-Mind"

Over the past year, the Department has made important strides in enhancing its force protection capabilities. But the job is not yet complete. A premier force protection capability will require continuous improvements in response to the changing strategic landscape. These recommendations will, in the panel's judgment, go a long way toward making US force protection capabilities sufficiently robust for dealing with the transnational threat.

ANNEX A.

Panel Membership

FORCE PROTECTION PANEL MEMBERSHIP

Co-Chairs

Gen Al Gray, USMC (Ret)*	
AMB. Henry Cooper	ARA

Members

COL Al DeProspero, USA (Ret)	
LtCol Michael Janay, USMC(Ret)	
Mr. John Kane	Sandia National Laboratory
Mr. Robert Moore	DST, Inc.
Mr. Lou Moses	RDA/Logicon

Government Advisors

COL Dan Baur, USA	DDOSD(I&S)(IWSCI)
LtCol James Carothers, USMC	USCENTCOM
BGen Jim Conway, USMC	J-34
BG Billy Cooper, USA	USCENTCOM/CCJR
Col Andy Corso, USAF	HQ AF/SFP
LtCol John Cowan, Jr., USMC	USMC-MCCDC
COL Dan Hahn, USA	J-34
COL Hal Johnson, USA	J-34 OPS
Mr. Paul Kozemchak	DARPA/ISO
Mr. Roberto Mata	ATSD(NCB)/CP
CAPT Arne Nelson, USN	OPNAV N312
COL Robert Neubert, USA	Army DCSOPS
LtCol Roby, USAF	AF/XOIIA
Mr. John J. Sloan	Defense Intelligence Agency
Mr. Dan Spohn	Defense Intelligence Agency

Contract Support

Ms. Barbara Bicksler	Strategic Analysis, Inc.

* Defense Science Board Member

ANNEX B.

Briefings and References

Briefings

From the time period of 21 April 1997 to 14 July 1997, the Force Protection Panel received the following briefings:

1. Department of Defense Antiterrorism/Force Protection Policy: Mr. James Q. Roberts, Principal Director, Policy and Missions, Office of Assistant Secretary of Defense for Special Operations/Low Intensity Conflict
2. J-34 Briefing to the Defense Science Board Force Protection Panel: BGen Jim Conway, USMC, Deputy Director for Combating Terrorism/Special Operations, J-34
3. Joint Staff Integrated Vulnerability Assessment: Col. Rick Kingman, Defense Special Weapons Agency
4. Combating Terrorism: Report from the Defense Advanced Research Projects Agency Tiger Team: Dr. Regina Dugan, Defense Advanced Research Projects Agency
5. Defense Intelligence Agency Office for Counterterrorism Analysis: Steve Scherer, Defense Intelligence Agency
6. Force Protection Activities at Sandia National Laboratories: John W. Kane, Program Manager, Weapons and CIS Security Programs, Sandia National Laboratory
7. Army Terrorist Threat Protection Research Program: Dr. Reed L. Mosher, US Army Engineer/Waterways Experiment Station
8. Air Force – Force Protection: Col. Gabe Buchholtz, USAF, Chief, Plans, Policy and Programs Division, Directorate of Security Forces
9. United States Navy, Chief of Naval Operations Antiterrorism/Force: CAPT Arne Nelson, USN
10. US Army Force Protection: LtCol Joseph Kamide, Army DCSOPS
11. US Marine Corps Force Protection Program Overview: LtCol Carlos Hollifield, USMC
12. Balanced Survivability Assessments/Vulnerability Assessments: Dr. Michael Shore, Springfield Research Facility, Defense Special Weapons Agency
13. CP Solutions to Terrorist Acts: Col. Ellen Pawlikowski, USA, OSD/Counter Proliferation
14. National Reconnaissance Office, Data Fusion Facility: Col Kip Hunter, USAF
15. Joint Physical Security Equipment Program (JPSE): Mr. Mike Toscano, Office of the Under Secretary of Defense for Acquisition and Technology
16. Technical Support Working Group: Mr. Jeff David, Office of the Secretary of Defense for Special Operations and Low Intensity Conflict

17. Force Protection, US Central Command: LtCol James P. Carothers, USMC, US Central Command
18. Organizational Change and Force Protection: Mr. Jim Locher, National Defense University
19. Antiterrorism/Force Protection: CNO Force Protection Briefing: CAPT Arne Nelson, USN
20. Terrorism and Counter-Terrorism: Implications for the USAF: Dr. Ian O. Lesser, RAND
21. Installation Risk Management Application (IRMA): Bryan Ware, SONALYSTS
22. Intelligence Observations: Mr. Dan Spohn, Defense Intelligence Agency
23. U.S. Armed Forces: Premier in Force Protection: Mr. John Kane, Sandia National Laboratories
24. Determining Requirements for Technology-Related Capabilities in Support of Force Protection: Mr. Lou Moses
25. Joint Staff Integrated Vulnerability Assessment Lessons Learned: Col Rick Kingman, Defense Special Weapons Agency
26. Combating Terrorism Overview – Downing Findings Status: COL Hal Johnson, J-34, Operations and Intelligence
27. Report from Threats and Scenarios panel: Mr. Gordon Negus
28. S&T Planning and DTOs for Force Protection: Dr. Jasper Lupo, Director, Defense Research and Engineering, Sensors, Electronics, and Battlefield Awareness
29. Air Force Force Protection: Col Andy Corso, USAF, Chief, Force Protection Division, Directorate of Security Forces
30. Air Force Corporate Investment in Force Protection: Col Andy Corso, USAF,
31. USAF Force Protection Technology: Col Andy Corso, USAF
32. CNO Force Protection Technology FY 98 RDT&E Efforts: CAPT Arne Nelson, USN
33. US Army Force Protection Budget : COL Robert Neubert, USA
34. US Marine Corps Force Protection Budget: LtCol Street, USMC
35. CBT Readiness Initiatives Fund: COL Hal Johnson, USA, J-34

References

1. *Combating Terrorism: Status of DoD Efforts to Protect Its Forces Overseas*, General Accounting Office GAO/NSIAD-97-207, July 1997.
2. CJCSI 5261.01. Combating Terrorism Readiness Initiatives Fund, March 1997.
3. *Critical Foundations: Protecting America's Infrastructures*, The Report of the President's Commission on Critical Infrastructure Protection, October 1997.
4. DoDD 2000.12, *DoD Combating Terrorism Program*, September 15, 1996.
5. "Defending the Troops," Peters, Katherine McIntire, Government Executive, April 1997, pp.39-42.
6. *Force Protection and Physical Security Equipment* – Technology Guide, June 1997.
7. *Force Protection Assessment of USCENTCOM AOR and Khobar Towers*, Report of the Downing Assessment Task Force, 30 August 1996.
8. *The Khobar Towers Bombing Incident*, House National Security Committee Staff Report, 14 August 1996.
9. *Joint Vision 2010*, The Joint Chiefs of Staff.
10. *Low Technology Approaches to Deflect Terrorism*, Col Paul Churchill Hutton, III, Ret.
11. *A National Security Strategy for a New Century*, The White House, May 1997.
12. *The National Security Threat of the 21st Century: Terrorist Use of Weapons of Mass Destruction Against the United States*, Lawrence Livermore Study Group, Lawrence Livermore National Laboratory, March 1997.
13. *Presidential Decision Directive-39-US Policy on Counterterrorism* - White House, June 1995.
14. *Report from Threats and Scenarios Panel* – Gordon Negus.
15. RDT&E Budget Justification Sheet.
16. Secretary of Defense Report to the President, *The Protection of US Forces Deployed Abroad*, September 16, 1996.
17. Technology Support to Counterterrorism Program/Budget Requirements Capability Requirements and Technology Support Matrix, Mr. Lou Moses, RDA/Logicon.
18. *Transforming Defense: National Security in the 21st Century*, Report of the National Defense Panel, December 1997.
19. Vulnerability Assessment Trends – USCENTCOM.

ANNEX C.

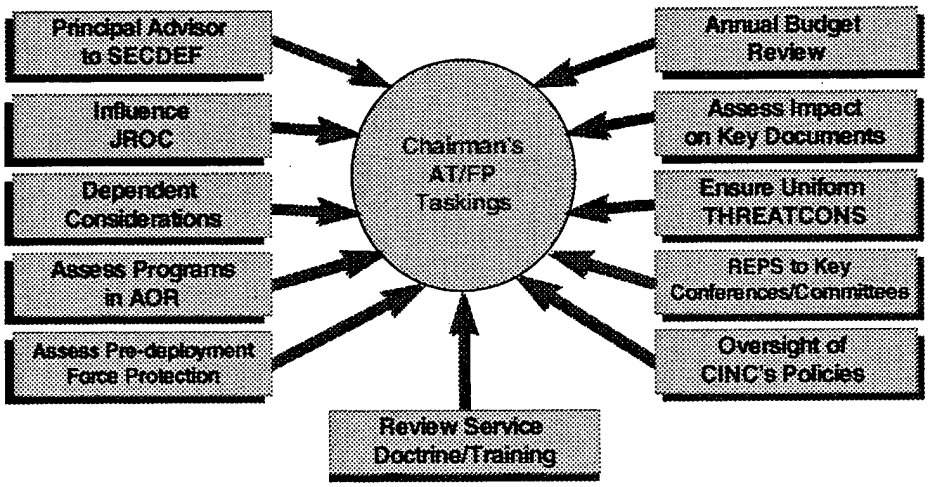
J-34 Force Protection Program

This Annex contains an overview of the Joint Staff, J-34 antiterrorism and force protection program, as well as details on the activities of each of the J-34 divisions: Plans and Policy; Operations and Intelligence; Training, Doctrine & Assessments; and Programs and Requirements.

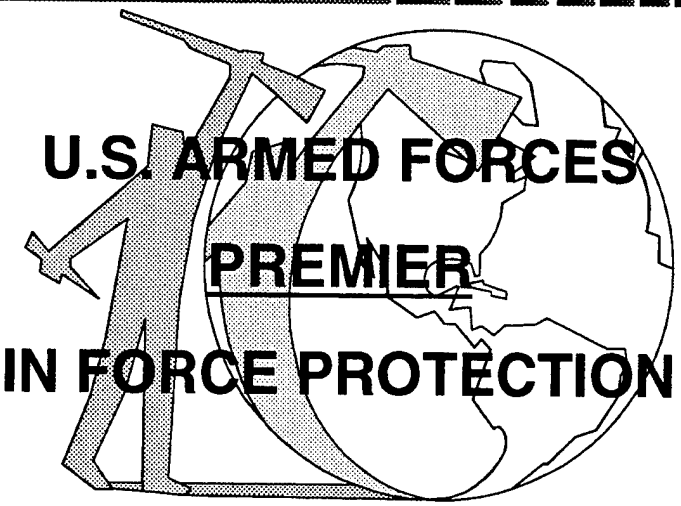
BGen Conway
Joint Staff/J-34

Chairman's Tasks

From DoD Combating Terrorism Program (DoD 2000.12)



Chairman's Vision

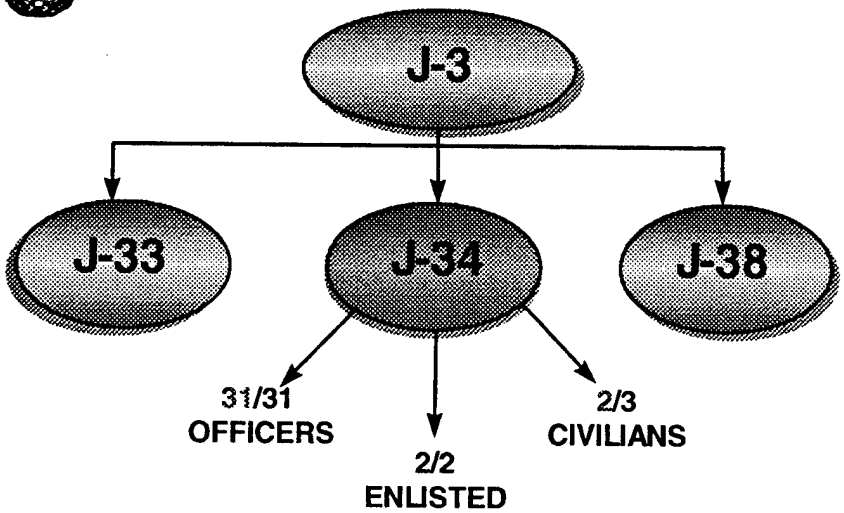


U.S. ARMED FORCES

PREMIER

IN FORCE PROTECTION

Cb-T Deputy Directorate



J-34 Mission

SUPPORT THE CHAIRMAN AND THE JOINT STAFF IN MEETING THE NATION'S SECURITY CHALLENGES AS THEY RELATE TO COMBATING TERRORISM, NOW AND INTO THE NEXT CENTURY.

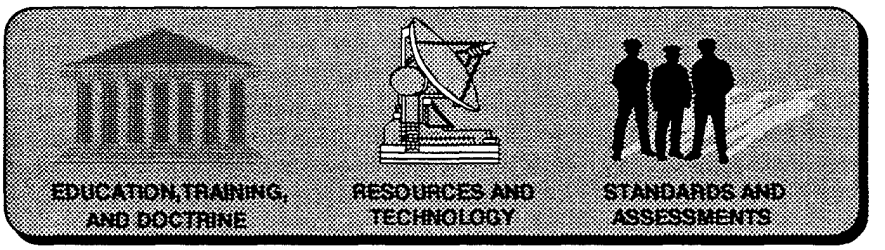
J-34 Objectives

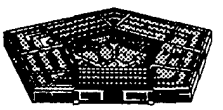
- To provide the CJCS unity of effort in dealing with all matters of combating terrorism.
- To assist the CINCs/Services in the execution of their force protection responsibilities.
- To make available emerging technologies to combat terrorism.
- To develop a uniform approach to our doctrine, standards, education, and training on combating terrorism.
- To enhance coordination with our allies in combating terrorism.

Downing TF Report

- A Road Map for DoD AT/FP Efforts
- Report Implementation
  - 26 findings / 81 actions
  - 100% complete
  - 1 action SECDEF rejected
  - 1 action CJCS redefined

Areas of Emphasis

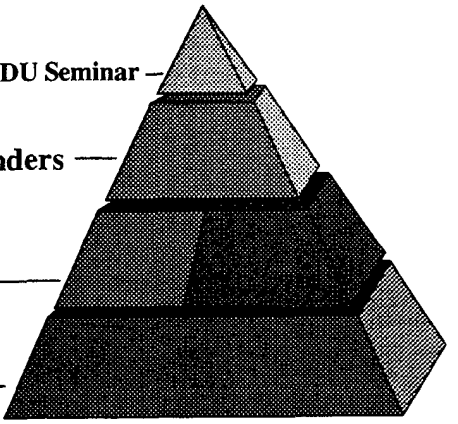




POLICY COORDINATION

OPERATIONAL FUSION

AT Training Concept



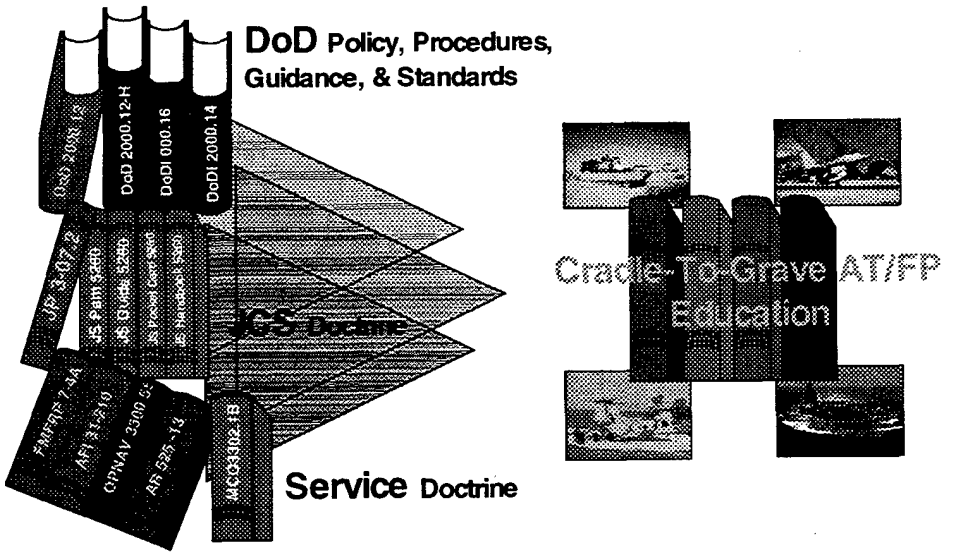
Level 4 --Senior "Executive" - NDU Seminar

Level 3 --Leadership - Commanders

Level 2 -- "Train the trainer" for unit AT/FP Trainer & Unit AT/FP R.O.

Level 1 -- Individual personal protection awareness

Doctrine & Education



Force Protection Technology

- CJCS Guidance: ..." *Engage American technology in the fight against terrorism"*
- 19 NOV 96 "Symposium with Industry"
  - Returns from Contractors
  - "On-Line" Catalog for CINCS/Services
- PSEAG and TSWG coordinate the technology integration
- 15-18 SEP FP Equipment demonstration @ Quantico

Joint Staff Integrated Vulnerability Assessments

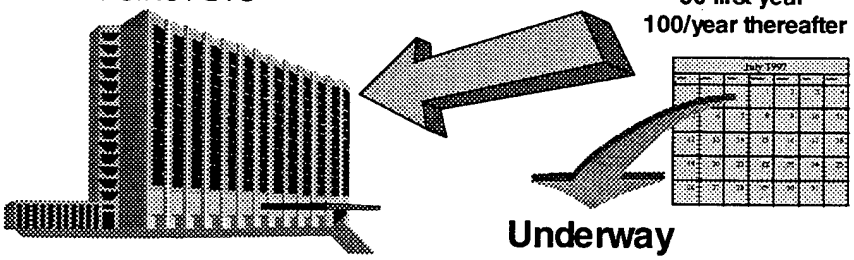
JSIVA TEAM

O-6 Team Chief
Security Specialists (x2)
Structural Engineer
Ops Readiness Specialist
"Terrorist Options" Specialist
Infrastructure Specialist
J-34 / DIA / CINC / SVS

5 Teams

Assessments

50 first year
100/year thereafter



Underway

Assessment Strategy

- 100 assessments per year (50-1st)
- Allocated by CJCS to CINCS and Services based on total number of facilities and percentage in high threat areas
- Scheduled by CINC/Service HQ
- Reports to Facility Commander and to CINC/Service Chief
- Trends and lessons learned to J-34 (JULLS, GCCS homepage)
- JSIVA Contact Team available to assist with problem areas

Installation /Threat Distribution

	NEG	LOW	MED	HIGH	TOTAL
ACOM (OCONUS)	4	2			6
CENTCOM		1	2	48	51
EUCOM	5	55	4	11	75
PACOM	3	58			61
SOUTHCOM		8		1	9
ARMY (CONUS)		138			138
USMC (CONUS)		18			18
NAVY (CONUS)		124			124
USAF (CONUS)		84			84
TOTALS	12	488	6	60	566

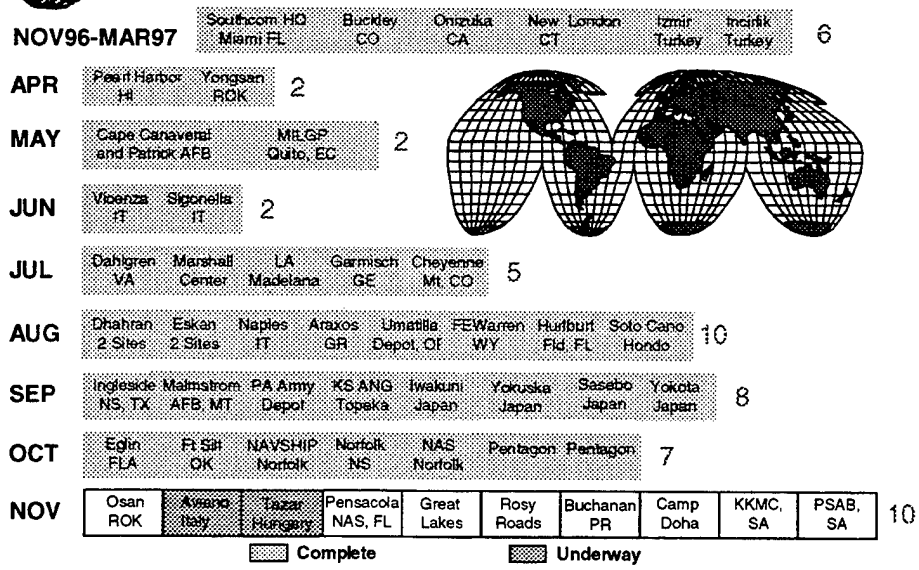
11/5/97 1

Installation Vulnerability Assessments

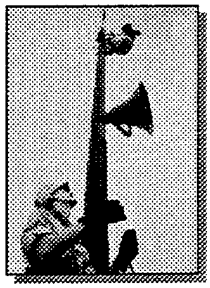
15 Sept 96 - 31 Dec 97

	NEG	LOW	MED	HIGH	TOTAL
ACOM (OCONUS)	4	2			6
CENTCOM		1	2	48	51
EUCOM	5	25/55	4	11	40/75
PACOM	3	16/58			16/61
SOUTHCOM		8		1	9
ARMY (CONUS)		26/138			26/138
USMC (CONUS)		14/18			14/18
NAVY (CONUS)		26/124			26/124
USAF (CONUS)		7/84			7/84
TOTALS	4/12	125/488	6/6	60/60	195/566

JSIVA Schedule CY 97



CONUS / OCONUS Assessments



OCONUS: Generally, higher threat locations

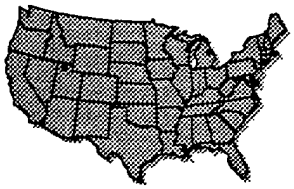
Emphasis on physical security measures

- A fully detailed assessment
- Objective: to avoid mass casualties
- Commanders must establish "acceptable risk"
- Security for troops - not cost - is the primary factor

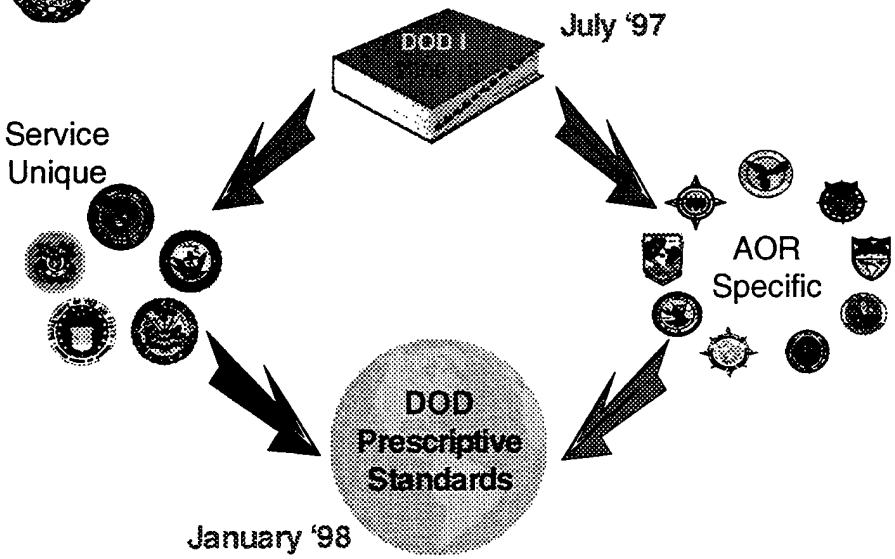
CONUS: Primarily Negligible/Low Threat

Emphasis on programs and procedures

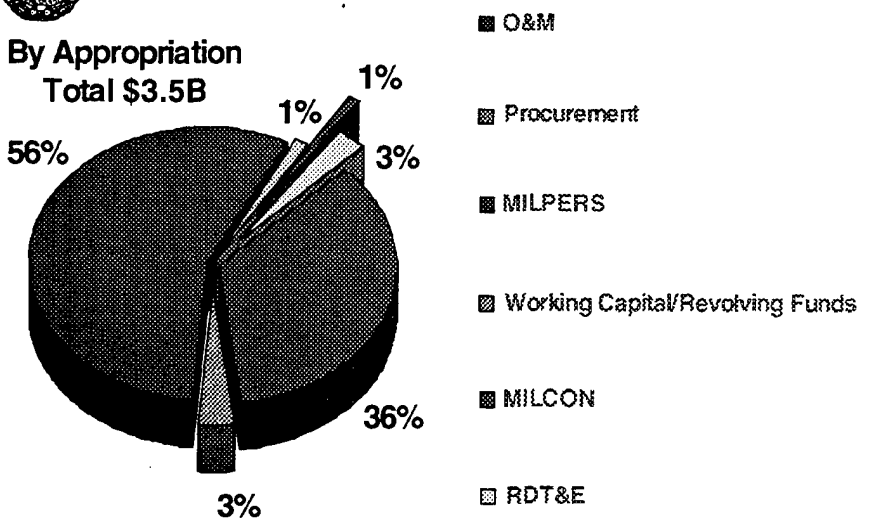
- Assessment teams are task organized
- Key: Can commander ramp up to THREATCON C or D ?
- Concept dependent on adequate warning
- Only affordable approach



Standards



FY98 Budget Submission - Combating Terrorism



Funding

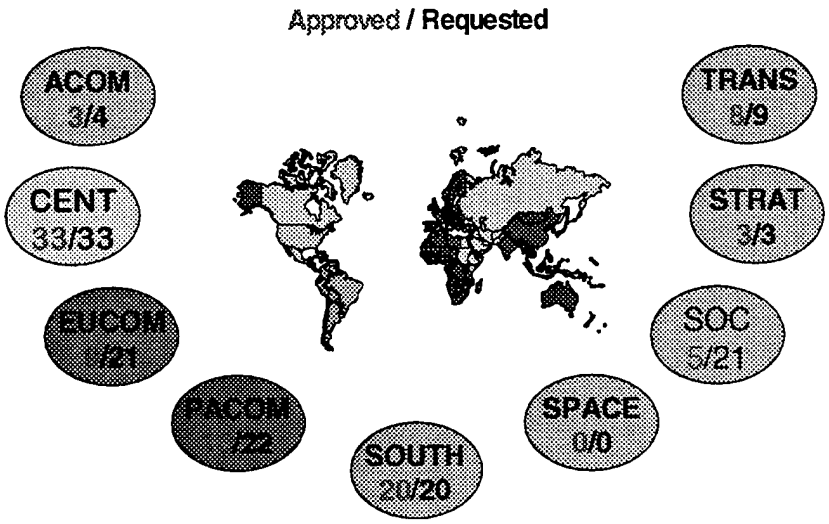
FY '97
$14M
+$10M

Chairman's RIF

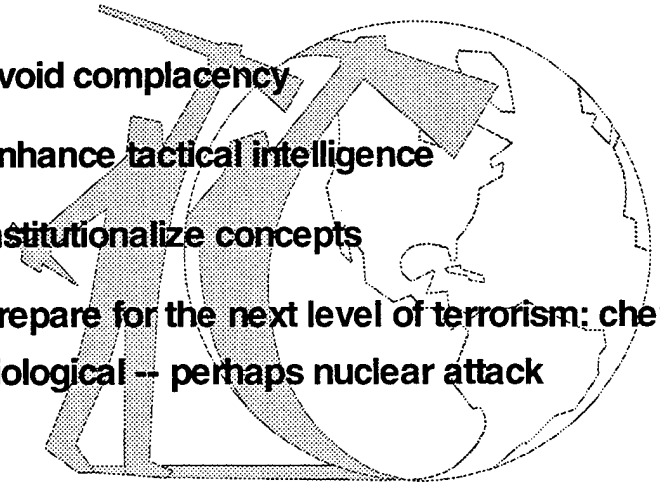
CINC	Obligations
ACOM	$3.817M
CENTCOM	$ .869M
EUCOM	$1.864M
PACOM	$2.324M
USFK	$2.495M
SOCOM	$1.486M
SOUTHCOM	$1.941M
SPACECOM	$1.118M
STRATCOM	$1.657M
TRANSCOM	$6.367M
TOTAL	*$23.94M*

FY '98-02
$15M

CINC Force Protection Personnel



Challenges



- Avoid complacency
- Enhance tactical intelligence
- Institutionalize concepts
- Prepare for the next level of terrorism: chemical, biological -- perhaps nuclear attack

J-34

PLANS AND

POLICY DIVISION

Col Steve Callicutt, USAF

Topics

- Manning
- Objective
- Policy Issue Update
  - DOD - DOS Force Protection MOU
  - MFO Sinai Force Protection
- JOPES Update

Manning

Division Chief	Col	Steve Callicutt
Plans / Policy	Lt Col	John Doolos
Plans / Policy / NBC	LTC	Al Hardy
Plans / Policy	LCDR	Paul Shigley
Policy Analyst	GS-13	Inbound
Summer Intern	Capt	Mark Lemery

Plans and Policy

OBJECTIVE

- **Coordinate AT/FP policy between OSD, Joint Staff, Geographic/Functional CINCs, Services, and DOD agencies**
  - **Monitor and participate in interagency process as appropriate**

Extension of 96 MOU - Worldwide

- **Issue**
  - Define FP responsibility for all DOD units and, where appropriate, transfer FP responsibility for DOD units currently under DOS for FP to the CINC
- **Background**
  - 96 MOU transferred Arabian Peninsula FP to CINC
  - DOS proposed worldwide expansion of 96 MOU; DOD (CJCS) proposed country by country approach
  - DOD proposed 20 countries/DOS 70
- **Status**
  - DJS message requires CINCs confirm the country list
  - DOS/DOD agreement on MOU language
  - Next step staff with State and EUCOM, CENTCOM, PACOM

MFO Sinai

- **Issue**
  - Put MFO under USCINCCENT FP using MOU process and "Forces For" Document
- **Background**
  - 1981: SECDEF designated Army as MFO Executive Agent until CJCS designated responsible CINC (never done)
  - 1986: Title 22 places non-CINC assigned forces under COM
  - '97 UCP: "Assign peacekeeping forces to CINC unless otherwise directed by NCA"
- **Status**
  - State attempting to maintain status quo
  - J34 submitting issue paper for "Forces For" Conference in AUG with CINCs and Service reps that would assign US forces in MFO to USCINCCENT

FP Update to JOPES

- Issue
  - Add Force Protection to Operation Order
- Background
  - JOPES Vol 2: Revised Jun 96 incorporates FP
  - JOPES Vol 1: Includes process and format for Warning, Planning, Alert, Deployment, Execute, and Operation Orders.
- Status
  - JOPES Vol 1: Interim Change incorporates FP.
  - Revised Vol 1, due out Dec 97, will retain Interim Change

J-34 Operations and Intelligence Division

Colonel Hal Johnson, USA

J-34 Operations and Intelligence Division

CENTCOM PACOM SOCOM SPACECOM USN USMC	EUCOM WHEM STRATCOM TRANSCOM USA USAF
Lt Col Mike Harris, USAF Maj Dave McKinley, USMC Maj Owen Devereux, USMC LCDR Pat Cleary, USN	LTC Bob Smith, USA Maj Steve Johnston, USAF Maj Tom Barrale, USAF

J-34 Operations and Intelligence Division

Daily Opns Requirements:

- Force Protection Concerns
  - CINC assigned forces
  - Non-CINC assigned forces
  - Peacekeeping forces
- Major terrorist groups within each AOR
- CINCs FP Organization and Initiatives
- Threat assessment information (AOR)
  - Threat Level
  - THREATCON

J-34 Operations and Intelligence Division

Goals and Objectives

- **Ops / Intel Fusion**
  - Continue to Build Strategy
  - Focus - Intra-Pentagon
    Inter-Agency
  - Engage Combatant Commands
- **Combatant Commands and Services**
  - Close Daily Coordination
  - Disseminate Information
  - Intel System Must Support Operators
- **Actively Engaged**
  - Assessments
  - Exercises
  - Conferences

J-34 Operations and Intelligence Division

Actions:

- **JRAC**
- **Downing Report**
- **Inter-Agency Intelligence Committee on Terrorism**
- **Coordination with NSA, FBI, DOS and USIA**
- **Defense Science Board**
- **Conventional War Plans**
- **SOUTHCOM HQ**
- **Intelligence**
- **"Guttenberg" (Chairman's FP Book)**

J-34

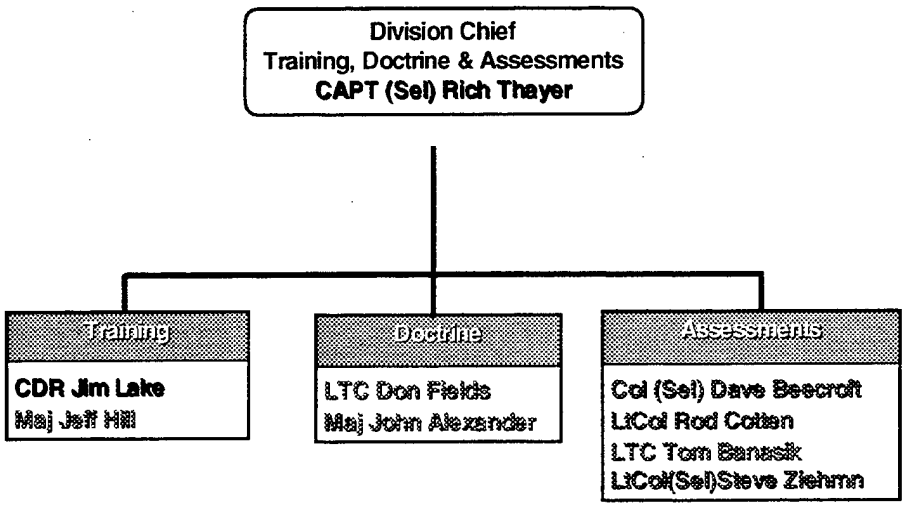
Training, Doctrine & Assessments Division

CAPT Rich Thayer, USN

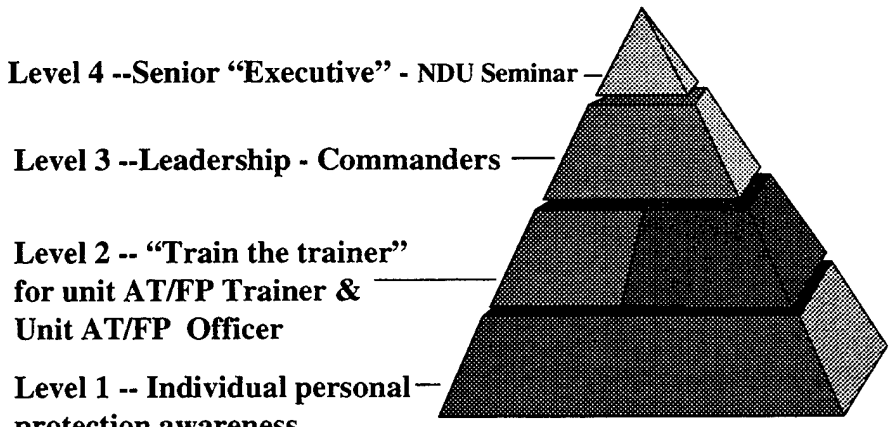
Topics

- Training
  - Training
  - Executive Seminar
  - Education
- Doctrine
  - JP 3-07.2
- Assessments
  - JSIVA Program

J-34 Organization
Training, Doctrine & Assessments Division

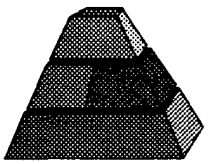


AT Training Concept



Executive Seminar

Level IV

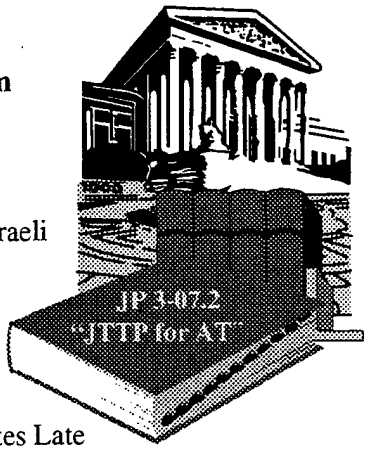


- Targeted at 0-6 to 0-8 level
  - Commanders, personnel responsible for AT/FP policy, planning and execution.
- 3 Day Seminar
  - Top-level Speakers, Panel Discussion, Wargame
  - J34 coordinates curriculum / current information updates
- First Seminar was conducted 22-24 Apr 97 at NDU
  - 52 attendees incl 8 flag officers
- Second Seminar will be 15-17 Sep 97 at ANSER, Crystal City
  - Will include 1/2 day at FP Equipment Demo, Quantico

Education

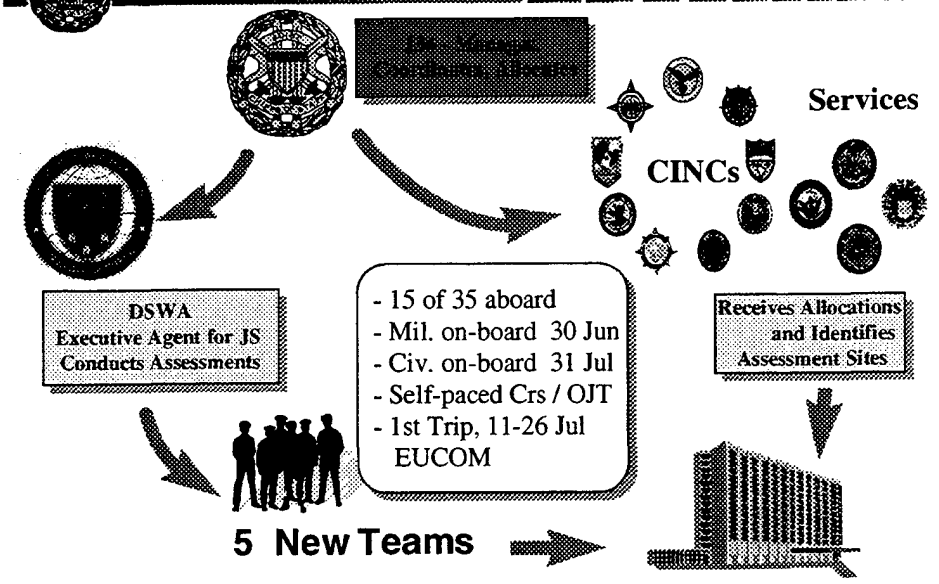
- Goal is Cradle-to-Grave AT/FP Education
  - In place: Off / Enlisted Accession training
  - Services determining intermediate off /enl education requirement
- Approved for inclusion in Intermediate and Top Level Schools
  - POI's under construction
  - partial implementation AY 97-98
  - full implementation AY 98-99

Doctrine



- **J34 - Doctrine Sponsor for Antiterrorism**
  - Lead role for rewrite
  - Working with J-7 and JDD at JWC
  - Will incorporate CINC/Service/UK and Israeli comments
- **Compressed Publication Goal**
  - 1st Draft to CINCs/Services/JS Directorates Late Summer 97
  - Final CJCS Approval Late Fall 97

JSIVA Assessment Program

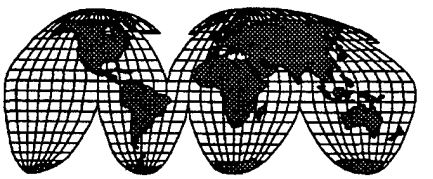


Assessment Methodology

- Concept for assessments
  - Combating Terrorism Vs. Mission
  - Avoidance of mass casualties
  - Three phases
    - Pre-visit info search
    - On site assessment
    - Report and post-visit assistance
- <u>Options</u> provided to commander
- Relies on "Acceptable Risk"

JSIVA Schedule

NOV96-MAR97	Southcom HQ Miami FL	Buckley CO	Onizuka CA	New London CT	Izmir Turkey	Incirlik Turkey			6
APR	Pearl Harbor HI	Yongsan ROK							2
MAY	Cape Canaveral and Patrick AFB	MILGP Quito, EC							2
JUN	Vicenza IT	Sigonella IT							2
JUL	Dahlgren VA	Marshall Center	LA Madelana	Garmisch GE	F.E. Warren				5
AUG	Prince Sultan	Eskan Village	Naples IT	Araxos GR	Umatilla Depot, OR	Gr Forks AFB, ND	Minot AFB, ND	SOUTH COM	8
SEP	R.Roads PR	Malmstrom AFB, MT	Buchanan PR	PA Army Depot	KS ANG Topeka	Iwakuni Japan	Yokuska Japan	Sasebo Japan	Kadena Okinawa	9
OCT	CENT COM	CENT COM	Eglin AFB, FL	San Diego CA	N. Island CA	Site "R"	China Lake CA	Ft Sill OK	Ft Detrick MD	9
NOV	Osan ROK	Aviano Italy	Eucom TBD	Pensacola NAS, FL	Corpus Christi TX	Crane IN	CENT COM	CENT COM	CENT COM	9



OCONUS Assessments

Generally, higher threat locations

- Emphasis on physical security
- Accurate threat analysis key
- Examines Ops/Intel interface
- Options briefed to commander; report provided
  - Current status of installation
  - Range of options to improve (procedural/programmatic to technical)
  - Possible implementation plans

CONUS Assessments

Primarily Negligible/Low Threat

- Emphasis on programs and procedures
- Task organized team
- Credibility a factor
- Options briefed to commander; report provided
  - Same as OCONUS

Concept dependent on adequate warning!
Only *affordable* approach

J-34

PROGRAMS AND

REQUIREMENTS DIVISION

Col Mike Hicks, USMC

Topics

- Manning
- Mission Area Analysis
- Technology Update
- Force Protection Equipment Demonstration Announcement
- Combating Terrorism Readiness Initiatives Fund (CbT RIF) Update

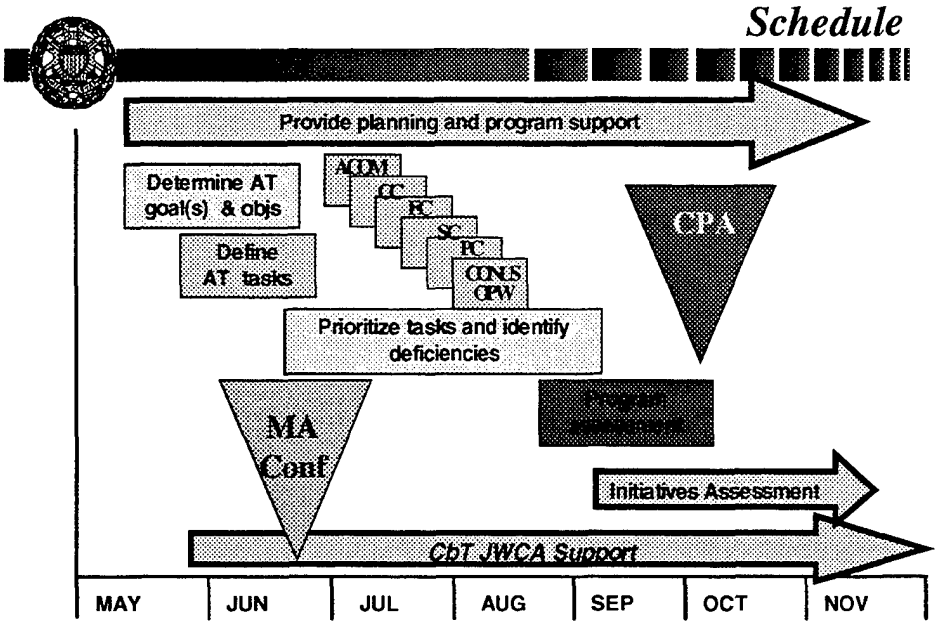
Manning

Division Chief	*Col.*	*Col. M.K. Hicks*
Sr. Program Off.	*LtCol.*	*LtCol. B.M. Nelson*
Mgt & Pgm	*GS13*	*Vacant*
Sr Reqmts Off.	*Maj*	*Maj. S. deCamp*
Sr Reqmts Off.	*LTC*	*LTC. V. Kam*
Sr Reqmts Off.	*LTC*	*LTC. J. Napier*
Sr Reqmts Off.	*Maj*	*Maj. E. Liberatore*

Mission Area Analysis

- **Purpose: Support JWCA milestones and input to the JROC -- - Chairman's Program Assesment (CPA)**
  - Address both materiel program elements and non-materiel issues
- **Who: P&R supported by ANSER Corp**
- **When: May - September 97**
- **How: Determine AT goals, objectives and tasks**
  - MAA conference
  - Operational Planning Workshops at CINC HQs to prioritize tasks and identify deficiencies
  - Program Assessment conference

Schedule



Force Protection Technologies

- Downing Report--"Technology was not widely used to detect, delay, mitigate, and respond to acts of terrorism."
- What We Need--
  - Commercial-Off-the-Shelf (COTS), Rapid Prototyping, Emerging Technologies
- Who Does It--
  - Physical Security Equipment Actions Group (PSEAG)
  - Technical Support Working Group (TSWG)
- Why--
  - Get Results Now--Put technology in hands of users
  - Service Acquisition Cycles too slow

Emphasis on AT/FP Equipment

- Two organizations received additional funds:
- PSEAG
  - COTS Testing
  - Added $5M in FY97, $12.6M for FY98 & FY99
- TSWG
  - Interagency group, DoD, DoS, FAA, FBI, DoE
  - Rapid Prototyping, Emerging Technologies
  - Added $17M for FY98, $19.2M for FY99

Force Protection Equipment Demonstration

- **SPONSOR: JS & USD A&T (PSEAG)**
- **OBJECTIVE:**
  - Provide DOD CINCs, commanders, other decision makers in military and civilian agencies of the Federal Government with opportunities to observe and become familiar with the latest in force protection equipment.

Force Protection Equipment Demonstration

- LOCATION: MCB Quantico, VA , Test Ranges and Demonstration Areas
- DATE: Sept 15-18,1997
- ADVERTISED: Announcement to contractors made in Mar 97 "Commerce Business Daily"
- DJCS msg 302359 Z April invited CINC and Services participation

Force Protection Equipment Display

Status

- 175 Firms (350 products) reviewed
  - 61 Firms received invitation letters and application packages
  - 19 firms received thank-you letters
- FPED home page on line 27 Mar (http://explorer.csc.com/fped)
- Public Affairs firm (Billcom) under contract effective 2 Apr 97

Equipment Categories

- Sensors Systems
- Surveillance Systems
- Barriers
- Explosives Detection
- Ballistic Resistant Equipment
- Blast protection and mitigation
- Cargo inspection devices
- Night Devices (thermal imaging, laser devices)
- Non-Lethal Weaponry

CbT Readiness Initiative Fund Update

- CJCSI 5261.01 effective 1 March 97
  - Distributed to CINCs and Services
  - Instruction also available on J-34 home page
- Fund was designed for high priority/urgent AT/FP requirements
  - CINCs/DCINCs may request through J-34
  - Instruction contains policy and procedures
  - Examples for fund use and request formats
- Sourced at $14M this year, $15M for FY98
  - Congressional supplemental - $10M for FY97

CBT READINESS INITIATIVES FUND

APPROVED FUNDING REQUESTS

ACOM	$255K	Vulnerability Assessments
PACOM	$100K	Vulnerability Assessment Study
STRATCOM	$ 30K	Vulnerability Assessments
SOCOM	$205K	AT/FP HQ Building Security
PACOM	$171K	AT/FP Equipment/Travel
TRANSCOM	$2.3M	AT/FP Equipment
CENTCOM	$974K	JRAC Start-up
PACOM	$ 8K	AT/FP Training
SOUTHCOM	$998K	AOR Assessments, Eqpt
SPACECOM	$533K	Onizuka, CA AT Security
TRANSCOM	$3.54M	AT/FP Equipment
TOTAL	*$9.1M*	

AS OF 20 JUNE 97

CBT RIF, continued

WORKING FUNDING REQUESTS

STRATCOM	$1.63M	HQ-AT/FP Security
TRANSCOM	$4.0M	AT/FP Eqpt for PAX Terminals
USFK	$1.3M	AT/FP Equipment, Upgrades
TOTAL	*$6.93M*	

PENDING FUNDING REQUESTS

CENTCOM	$1.3M	AT/FP Equipment
EUCOM	$6.6M	AT/FP Equipment
SOUTHCOM	$2.6M	HQ Security, AT/FP in Panama
ACOM	$2.8M	AT/FP Items for MARFORLANT
PACOM	$1.5M	AT/FP Items for MARFORPAC
ASSESSMENT RESULTS	$3.0M	JSIVAs Scheduled through 1 Oct
TOTAL	*$17.8M*	

GRAND TOTAL of all requests $33.8M (exceeds $14M FY 97 fund limit)
****$10M added to CBT Fund in Jun Supplemental Bill--new limit $24M****

AS OF 20 JUNE 97

Summary

- JWCA Trip - July 97
- Mission Area Analysis - Summer 97
- Technology Teams - May - August 97
- Force Protection Equipment Demo - Sept 97
- Guidebook - June 97

ANNEX D.

Service Force Protection Programs

This Annex contains an overview of the force protection programs in the Army, Navy, Air Force, and Marine Corps. The briefings include material on organization, requirements, and new and ongoing activities.

ARMY FORCE PROTECTION

- OVERVIEW
- ACCOMPLISHMENTS
- ONGOING INITIATIVES
- CHEM / BIO CONSIDERATIONS
- ASSESSMENT OBSERVATIONS
- REQUIREMENTS
- CHALLENGES
- SUMMARY

"Force Protection is the most difficult near-term challenge we face as an Army."

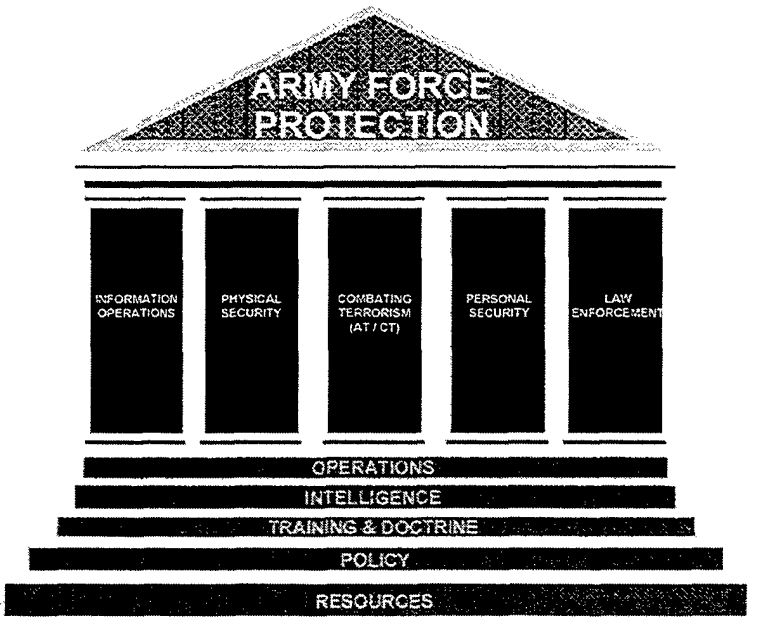
General Reimer, CSA
SLTC, July 1997

DEFINITION

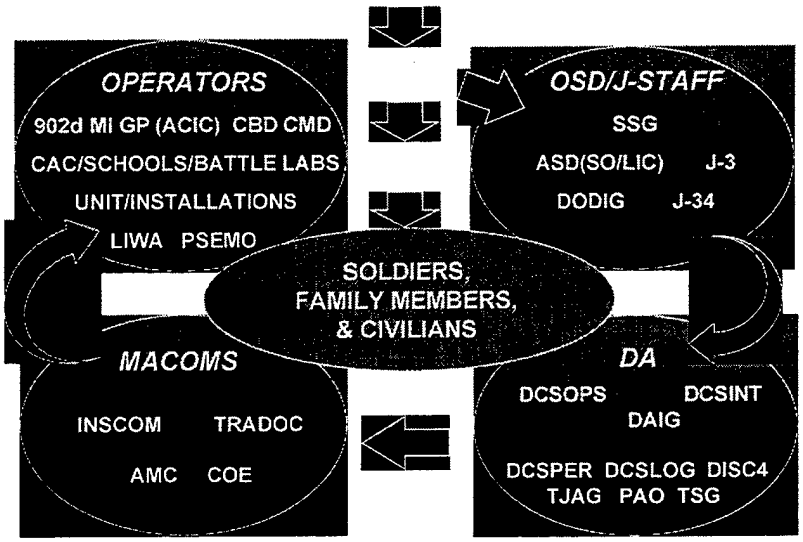
FORCE PROTECTION IS A SECURITY PROGRAM DEVELOPED TO PROTECT SOLDIERS, CIVILIAN EMPLOYEES, FAMILY MEMBERS, FACILITIES AND EQUIPMENT, IN ALL LOCATIONS AND SITUATIONS. THIS IS ACCOMPLISHED THROUGH THE PLANNED INTEGRATION OF ***COMBATING TERRORISM (AT / CT), PHYSICAL SECURITY, INFORMATION OPERATIONS, PERSONAL SECURITY*** AND ***LAW ENFORCEMENT OPERATIONS***, ALL SUPPORTED BY THE SYNCHRONIZATION OF **OPERATIONS, INTELLIGENCE, TRAINING AND DOCTRINE, POLICY AND RESOURCES.**

AR 525-13, THE ARMY FORCE PROTECTION PROGRAM

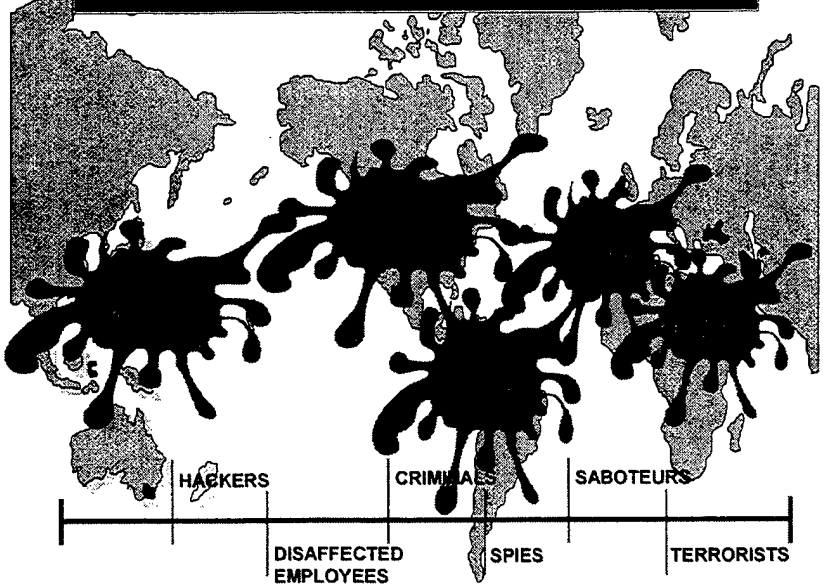
THE PILLARS



RESPONSIBILITIES



WORLDWIDE ENGAGEMENT
WORLDWIDE THREAT



CHANGE THE MINDSET

- ENEMIES ATTACK USING ASYMMETRICAL MEANS:
  - AVOIDS STRENGTH, ATTACKS VULNERABILITIES.
  - CASUALTIES ARE AN AMERICAN CENTER OF GRAVITY.
- IN THE PAST, FORCE PROTECTION EMPHASIS REACTIVE VS. PROACTIVE.
- FORCE PROTECTION IS A DISCIPLINE IN EVERYTHING, PLANNING THROUGH EXECUTION.
- POTENTIAL FOR HIGH CASUALTIES FROM A SINGLE ATTACK IS UP: LARGER BOMBS, POTENTIAL WMD.

ACCOMPLISHMENTS

POLICY

- DoD POLICY UPDATED
- DoD WORKING GROUPS
- DA POLICY UPDATED

OPERATIONS

- FP ASSESSMENTS
- FP STEERING COMMITTEE
- FP IN MILCON
- FP HOMEPAGE
- DoDWWATC
- ACERT OPERATIONAL
- EUROPE RCERT OPERATIONAL

RESOURCES

- EQUIP FIELDING
- LIWA FUNDED
- OPA PLUS-UP (99-00)

TRAINING & DOCTRINE

- LEVEL I-IV TRAINING

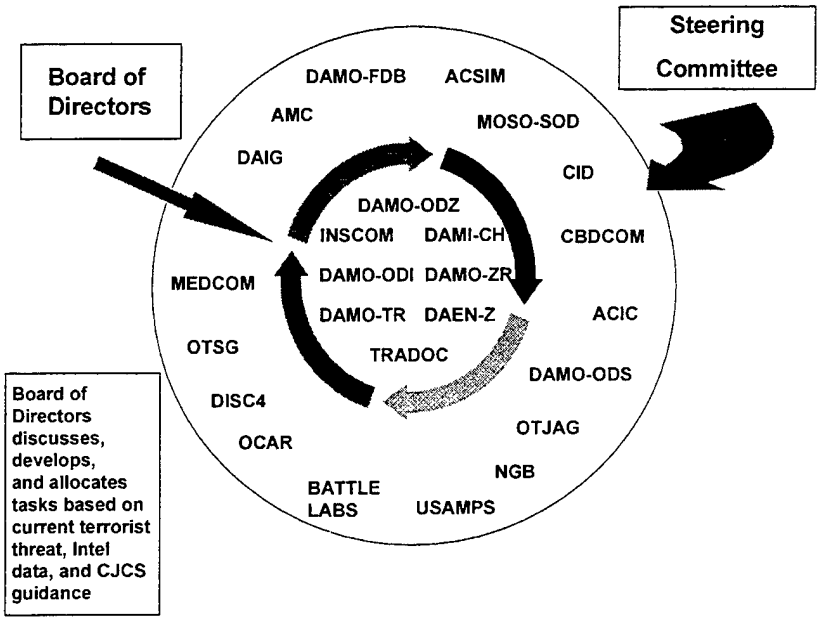
INTELLIGENCE

- THREAT ID SPT - MFO
- IPR ON TERRORIST THREATS
- CACTIS UPGRADES - ATOIC/ACIC
- CI FP SOURCE OPS TNG

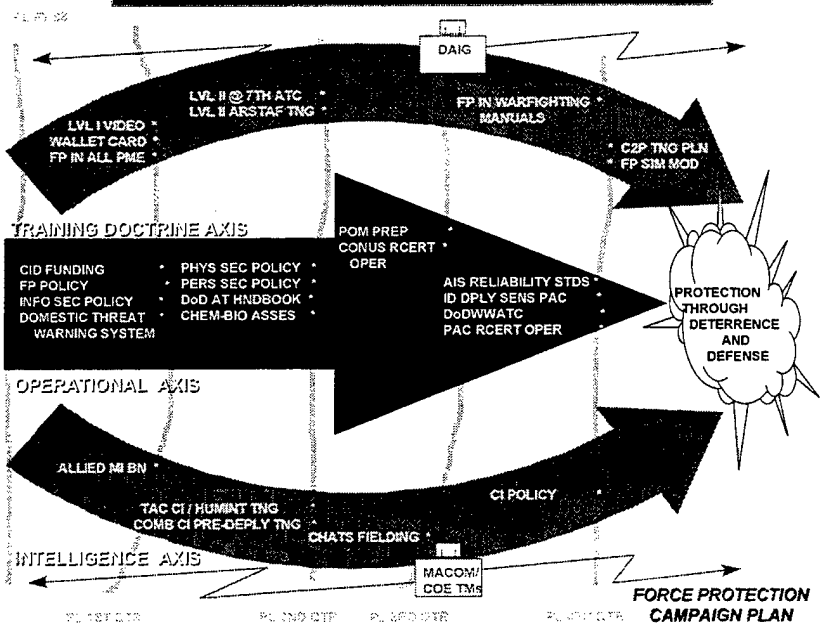
TECHNOLOGY

- DoD TECH GUIDE
- DoD FP EQUIP DEMO

STEERING COMMITTEE



ONGOING INITIATIVES



CHEM-BIO PROTECTION

MUST BE PART OF FORCE PROTECTION

CB TERRORISM
- LOW PROBABILITY
- HIGH CONSEQUENCE
- HIGH VISIBILITY INCIDENT

CONSEQUENCES ARE NOT ACCEPTABLE

CHEM-BIO PROTECTION INITIATIVES

CBDCOM WILL PROPOSE THE FOLLOWING TO HQDA FP STEERING COMMITTEE :

PROVIDE CB ASSESSMENTS AND ASSESSMENT TOOLS TO INSTALLATION COMMANDERS AND JCS ASSESSMENT TEAM

RECOMMEND TRADOC LEAD A MULTI-FUNCTIONAL TEAM TO INTEGRATE CB ENHANCEMENTS INTO ARMY FORCE PROTECTION

PROVIDE TRAINING MATERIAL TO TRADOC SCHOOLS FOR TRAINING OF INSTALLATION / COMMUNITY

PROVIDE EXERCISE SCENARIOS AND LESSONS LEARNED

PROVIDE CB FORCE PROTECTION BRIEF TO PCC AND GARRISON COMMANDER COURSE

ESTABLISH DOD CB HELPLINE AND WEB PAGE LINK

FRAMEWORK FOR CB FORCE PROTECTION

- RESPONSE FORCES TO BE TRAINED / EQUIPPED
  - FIRE & MILITARY POLICE
  - EMERGENCY MEDICAL
  - POST OPS CENTER
  - COMMAND STRUCTURE

- TERRORIST EVENT RESOURCE REQUIREMENTS
  - DETECTION, MONITORING, & DECON
  - INDIVIDUAL PROTECTION
  - COMMUNICATION
  - MEDICAL
  - COMMAND

ENABLERS

CHEMICAL SCHOOL
MP SCHOOL
CBDCOM
MEDCOM
SSCOM

ASSESSMENT OBSERVATIONS

(GENERAL)

- KNOWN THREAT + COMMAND EMPHASIS = GOOD PROGRAMS
- PERCEPTION OF NO THREAT + NO COMMAND EMPHASIS = WEAK PROGRAMS
- MACOM PROGRAMS NOT FULLY IMPLEMENTED AT INSTALLATION LEVEL
- INTEL SPT STRUCTURE PRESENT, SOMETIMES CONSTRAINED
- POLICY ADEQUATE - NOT UNIFORMLY APPLIED
- EXTERNAL EXPERTISE NOT FULLY UTILIZED

ASSESSMENT OBSERVATIONS

(SPECIFIC)

- ✕ ANNUAL FORCE PROTECTION EXERCISES NOT CONDUCTED
- ✕ NO FORCE PROTECTION COMMITTEE OR WORKING GROUP
- ✕ AIS USERS AND ADMINISTRATORS NOT TRAINED
- ✕ NO PROVISIONS TO CLOSE INSTALLATIONS
- ✕ PHYSICAL SECURITY EQUIPMENT INOPERATIVE
- ✕ FORCE PROTECTION OFFICER NOT TRAINED
- ✕ MANDATED INSPECTIONS NOT BEING CONDUCTED
- ✕ LEVEL I TRAINING NOT BEING CONDUCTED
- ✕ TENANT / SUPPORTED ACTIVITIES NOT INCLUDED IN PLANING OR PLANS
- ✕ NO PROVISIONS FOR WMD
- ✕ THREAT INFORMATION DISSEMINATION PROCEDURES NOT IN PLACE

FORCE PROTECTION REQUIREMENTS

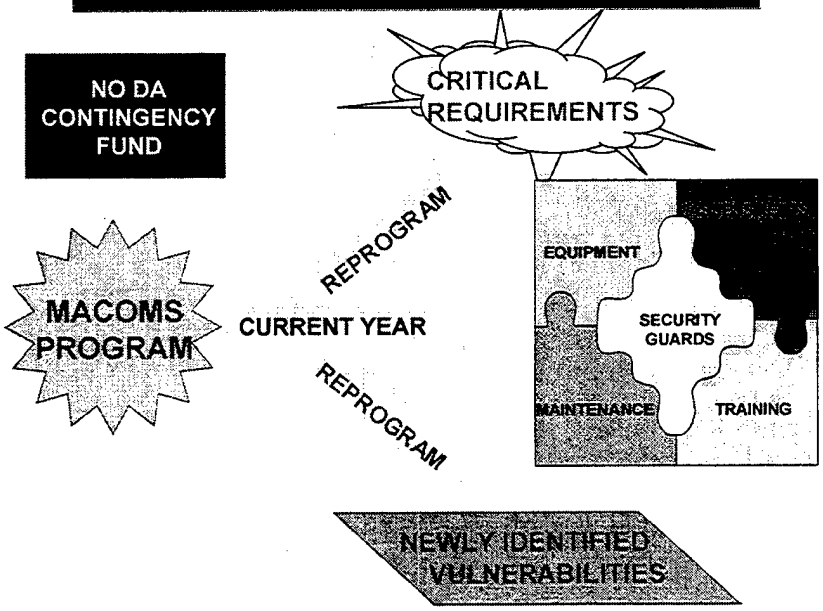
- ✓ PROGRAM BASED UPON THREATS AND VULNERABILITIES
  - ↳ COORDINATED AND INTEGRATED WITH HOST NATION, FEDERAL, STATE AND LOCAL LAW ENFORCEMENT
  - ↳ INCORPORATED IN PLANS / OPORDERS
- ✓ COMMITTEE AND WORKING GROUP
  - ↳ MEET PERIODICALLY
  - ↳ KEY STAFF PRINCIPLES
  - ↳ HEADED BY G3/DCSOPS
- ✓ ANNUAL COMPREHENSIVE FORCE PROTECTION EXERCISE
  - ↳ INCLUDES THREAT WMD AND AIS ATTACK
  - ↳ EVALUATES THREATCON, ATTACK WARNING SYSTEMS, AND CONSEQUENCE MANAGEMENT PLAN
- ✓ MACOM's REVIEW INSTALLATION PROGRAMS EVERY 3 YEARS
  - ↳ INTERNAL INSTALLATION REVIEW ANNUALLY
- ✓ APPOINTMENT OF FORCE PROTECTION OFFICER
  - ↳ ALL LEVELS, DOWN TO DEPLOYABLE BATTALION
  - ↳ TRAINED, CERTIFIED AND CURRENT

FORCE PROTECTION REQUIREMENTS

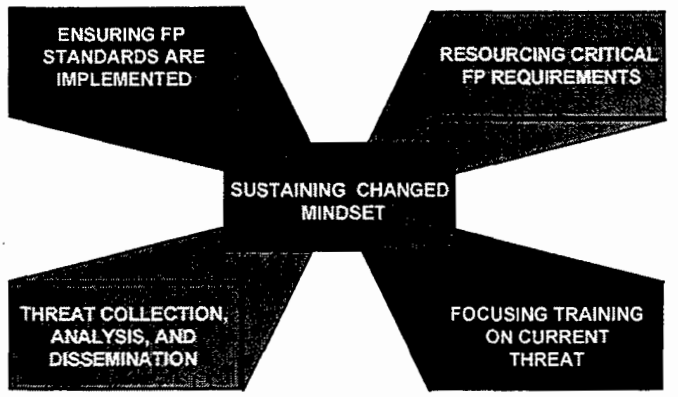
(cont)

- ✓ COLLECT, RECEIVE AND DISSEMINATE THREAT INFORMATION
  - ↳ CONNECTIVITY WITH FEDERAL, STATE AND LOCAL LAW ENFORCEMENT
  - ↳ AFTER DUTY HOURS PROVISIONS
  - ↳ SUPPORTED TENANT / RC COMPONENTS INCLUDED
- ✓ THREAT AND VULNERABILITY ASSESSMENTS
  - ↳ ADDRESSES ENTIRE SPECTRUM OF THREATS
  - ↳ COMPREHENSIVE LOOK (MI, MP, ENG, CHEM)
  - ↳ DISSEMINATED TO AFFECTED ACTIVITIES
- ✓ LEVEL I TRAINING
  - ↳ 6 MONTHS PRIOR TO TRAVEL OCONUS
  - ↳ MILITARY, DA CIVILIAN AND FAMILY MEMBERS
- ✓ RESOURCE MANAGEMENT
  - ↳ BASED UPON THREAT, VULNERABILITIES AND RISK MANAGEMENT
- ✓ SECURITY ENGINEERING AND PLANNING
  - ↳ FP CONSIDERED IN ALL MILCON

RESOURCES



CHALLENGES



SUMMARY

- PROGRAM IN EFFECT -- *INSTITUTIONALIZE STANDARDS*
- THREATS TO THE ARMY WILL CONTINUE
- FORCE PROTECTION IS *EVERYONE'S* RESPONSIBILITY (CDR'S, STAFF, SOLDIERS, FAMILIES, CIVILIANS)
- TRAINING AND COMMAND EMPHASIS MUST INSTILL FORCE PROTECTION AS AN ELEMENT OF DISCIPLINE FROM PLANNING THROUGH EXECUTION
- FOCUSED EFFORT IS THE KEY

FP ENABLERS

EQUIPMENT

- AMC QUICK RESPONSE OFC
  - -- LTC HOUSE
  - (703) 617-5790/4640
- PHYSICAL SCTY EQUIP MGMT OFC
  - LTC SWAGLER
  - (703) 704-2416/2412

ENGINEERS

- PROTECTIVE DESIGN CTR
  - MR WEHRING
  - (402) 221-3817/4918
- ELECTRONIC SEC SYS CTR
  - MR BROWN
  - DSN 760-1756

POLICY

- ODCSOPS (DAMO-ODL)
  - LTC KAMIDE
  - DSN 225-8491/8492

COUNTERINTELLIGENCE

- POLICY
  - COL MCGILL
  - DSN 225-8911
- THREAT
  - ATOIC
  - DSN 227-5484/5485
  - ACIC
  - DSN 923-3409

TRAINING & DOCTRINE

- TRADOC
  - COL ANCKER
  - DSN 552-4879

NAVY COMBATING TERRORISM PROGRAM

CNO N31 Mission and Objectives

- **Provide CNO unity of effort.**
- **Support the Fleet CINCs and other Echelon 2 commands in Combating Terrorism.**
- **Develop a uniform approach to doctrine, standards, education and training.**
- **Single point of contact coordinating with the Joint Staff, other Services and Interagency.**

NCIS Contribution

AT / FP: Center of Expertise

- LEPS / AT / Engineering / Systems Support and Protective Design
- CNO Integrated Vulnerability Assessment Teams
- NCIS Mobile Training Teams: Security force training ashore and afloat

Counterintelligence: Center of Expertise

- NAVATAC: all source AT fusion cell
- NCIS CI Agent at every Navy Base / CVBG / ARG

Navy Success in AT Awareness and Training

CNO Tasks

from CbT program DoDD 2000.12

Successes

TRAINING

- **400 unit FPOs / 2000 unit ATTOs (ongoing MTT / fixed site)**
- **All levels underway: Accession, PCO/PXO, Senior Leader**

FUNDING

- **Established, via PBD-98C, Priority Funding for OCONUS ESS Installation and Maintenance (FY 98 $27.8M)**
- **Agreed, via PR-99, to Fund ESS Hardware Installations and Maintenance and Hold the Line on Manpower (FY99 $18.1M)**

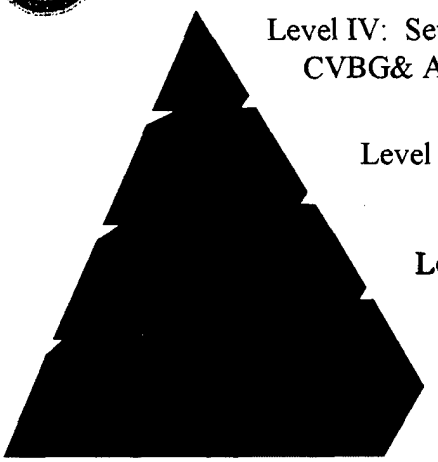
TECHNOLOGY / R&D

- **Waterside Security System and Entry Control Screening and Explosive Detection Systems in place Bahrain**
- **Navy Labs involved in Blast Mitigation / Explosive Detection**

NAVY INTEGRATED VULNERABILITY ASSESSMENTS

- **11 CNOIVA / 5 JSIVA complete**

AT Training Concepts



Level IV: Senior Executive Course
CVBG& ARG - CDRS/COS/N3

Level III: PCO/PXO Leadership

Level II: Unit FPO/ATTO

Level I: Individual/Personal
Protection Awareness

Publications/Standards

DoDD 2000.12 ➡ Policy ➡ OPNAVINST 3300.53

DoDD 2000.12H ➡ Guidance ➡ OPNAVINST 3300.54

DoDD 2000.16 ➡ Standards ➡ (P) OPNAVINST 3300.55

DoDD 2000.14 ➡ Procedures ➡ (P) OPNAVINST 3300.56

☑ DoD Pubs issued as OPNAVINSTs to Ensure Dissemination at Unit Level

☑ Expect Late Summer 97 Target Date

FP Funding

- Current Budget: O&MN $270M / MILPERS $270M
  - 90%: salaries / 10%: Day to Day Operations (maintenance, comms, vehicles, training, travel, ESS, intrusion systems for MILCON, procurement, and R&D)
  - MILCON: (98) $25M / (99) $31M Bahrain Barracks
- Need Modernization/Investment Capital
  - Minimal Modernization Funding
  - Need Investment Capital (comms, screening devices, ESS) and Improved Technology Systems

Modernization / Capitalization

- Screening Devices: Baggage Scanners, Explosive/ Metal Detection
- Security Force Equipment: APCs, Mobile Firing Ranges, Body Armor, MWD teams
- Electronic Security Systems: Thermal imaging, CCTV, Intrusion Detection, Access Control, Monitor/Control Equipment
- Communications Equipment: Digital Encryption Radios, Trunking Systems, Base/Mobile Systems

Technology
FY 97-98 RDT&E Efforts

- Waterside Security (NRAD): Swimmer Detection sonar
  - NSB Kings Bay, ASU Bahrain, NSB New London
- Shipboard Physical Security Program (NSWC Crane):
  - CCTV, digital recording/biometrics, lighting. Baseline development for CVN-76
- Portable Explosives Detection (EODTD, Indian Head)
  - New system, no COTs available
- Entry Point Screening (EODTC, Indian Head):
  - Multisensor truck entry point detection, ASU Bahrain
- Building Hardening Techniques (Port Hueneme):
  - Glazing and blast mitigation efforts

Assessment Strategy

DoD Standard: "Evaluate AT/FP vulnerability and make subsequent recommendations to improve Force Protection posture." All installations to be assessed within a 3 year period.

- **FY 97 17 CNOIVA / 10 JSIVA**
- **FY 98 20 CNOIVA / 17 JSIVA**

- **OCONUS: emphasis on Physical Security posture.**

- **CONUS: Risk Management--emphasis on programs and procedures, ramp up to Threatcon "C".**

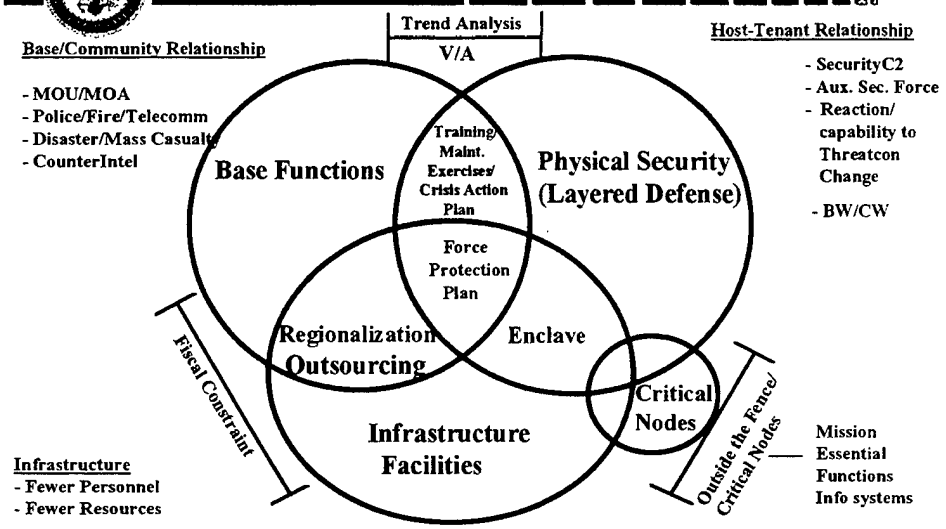
A Strategic Plan: Assumptions

- **Requirements seem Infinite, Resources are Finite**

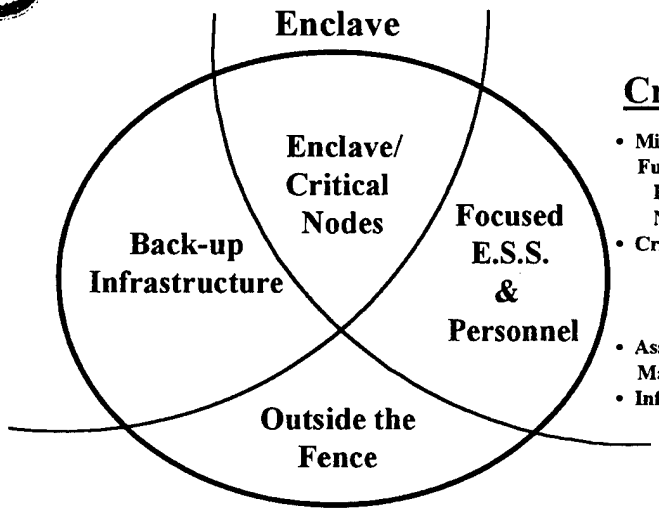
- **Decisions outside Commander's Control**
  - **Resources**
  - **Manpower Reductions**
  - **Infrastructure Reductions**

- **Decisions within Commander's Control**
  - **Outsourcing**
  - **Enclave (mission critical functions)**
  - **Layered Defense**
  - **Unit Force Protection Plan**

FP Long Range Base Strategic Plan
(CRITERIA AND VALIDATION)



Critical Nodes and Assets



Critical Nodes

- Mission Essential Functions
  - High Value
  - National Assets
- Critical Infrastructure
  - Communications
  - Power
  - Transportation
- Assembly / Marshalling Areas
- Information systems

VA Trends

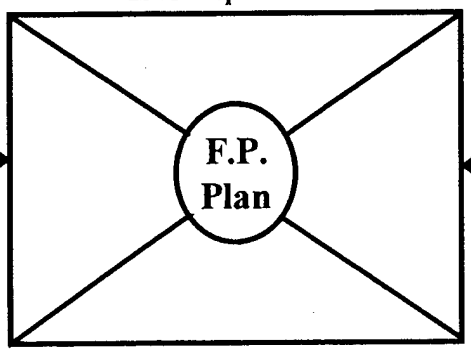
11 CNOIVAs / 5 JSIVAs through 31 July 1997

- **Policy**
  - **FP Policy and Open Base Policy under review**
  - **FP Funding competes with other important programs (QOL)**
- **Perception**
  - **Threat Negligible, therefore Risk Low**
- **C2**
  - **Blurred Organizational Lines of Authority**
  - **Out of Date Communications Systems**
- **Program Management**
  - **FP Master Plan Out-of Date / No modernization plan**
- **Training/Exercises**
  - **Inadequately Trained Security Force / Auxiliary Security Force**
  - **Crisis Action Plan not Exercised**

Ship Force Protection Plan

Top Down
- **CNO IG Special Interest Item**
- **ISIC Inspection**

- Mission
- Ops
- Location
- Intel
- Port Security
- Threat Level



- Standards
- Training
- Maintain Equip
- Exercise CAP
- Procedures
  - Explosive
  - Antiswimmer
  - C/B Defense
  - Mass Casualty
- Tech. Initiatives

Bottom up
- **Certification Program/ISIC**
- **Self Assessment**

Challenges

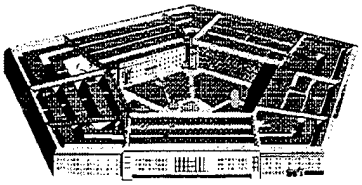
- Change in Mindset--Institutionalize AT/FP in Naval Operations
  - Long Term vs. Trend
  - Not Just Another Program
  - Not Someone Else's Job

- Re-emphasize an Existing Program

- Prepare for Next Level of Terror: Chem/Bio/Nuc/Info

- Force Protection is a QUALITY OF LIFE Program
  - FP is a Quantity of Life Program and
  - Quantity has a Quality all its own

Air Force -- Force Protection



Defense Science Board

Colonel Gabe Buchholtz
Chief, Plans, Policy and Programs Division
Directorate of Security Forces

Air Force -- Force Protection

Air Force -- Force Protection

*"... the Khobar Towers attack should be seen as a watershed event pointing the way to a **radically new mindset and dramatic changes** in the way we protect our forces deployed overseas from this growing threat." (15 Sep 1996, Report to President)*

"... we can't be the best at building airplanes and submarines and second or third best at protecting our men and woman." (19 Nov 1996, Defenses Special Weapons Agency Conference)

Air Force -- Force Protection

Joint Force Protection Efforts

- **OASD(SO/LIC) Senior Steering Group**
  - **SF, XO**
- **OASD (SO/LIC) Antiterrorism Coordinating Committee**
  - **SF, IN, XO, OSI, IGX**
- **FP Joint Warfighting Capabilities Assessment (JWCA)**
  - **SF, OSI, IN, XO**
- **J-34 Combating Terrorism Staff**
  - **SF, OSI, XO, specialties assigned**
- **New DIA Counterterrorism Center at Bolling AFB with CT/AT focus**
  - **Provides fusion and assessment to all levels**
  - **OSI is AF representative**
  - **Streamlines intelligence/counterintelligence structure**

CSAF FP Implementation Message

- 15 Nov 96 Message Directed the Air Force to:
  - Restructure the Air Staff to provide Force Protection focal point
  - Develop Force Protection field organization (820th Security Forces Group)
  - Expand guidance to air component commands
    - Staffs, Tour-lengths and Training
  - Coordinate with Joint Staff to expand ROE for countries without status of forces agreements
  - Instill FP awareness at all levels of the AF

Air Force -- Force Protection

CSAF Implementation Message (Cont)

- Support the streamlined Intel and Counterintelligence structure for JTF-SWA
- Review the dissemination of counterintelligence/ antiterrorist information to FP officials
- Establish Force Protection Battle Lab
  - Develop requirements for surveillance systems
  - Explore applications of off-the-shelf alert systems

Force Protection Organizations

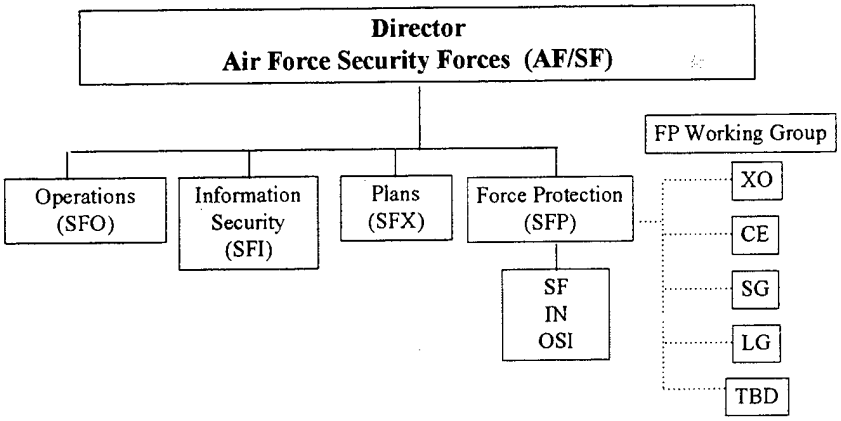
- Air Staff Force Protection Division
- Air Force Security Forces Center
- 820th Security Forces Group
- Force Protection Battle Lab

Air Staff Force Protection Division

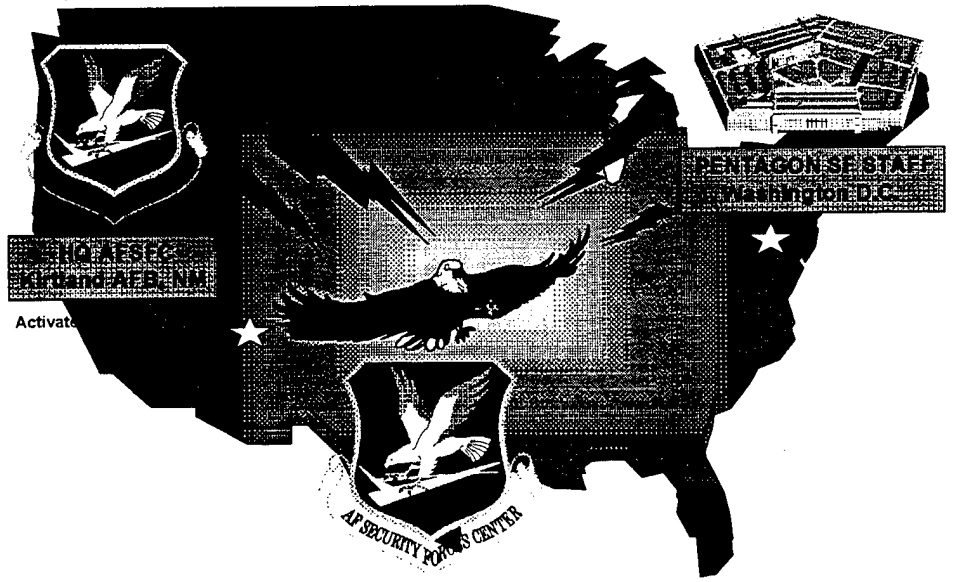
- New division led by an O-6 under the Director, Air Force Security Forces
- Provides force protection resource advocacy, policy, and guidance to the field
- Composed of Security Forces (SF), Intelligence (IN) and Office of Special Investigations (OSI) resources and matrixed with other Air Staff organizations as necessary
- Organization stood-up 1 Jan 97

Air Force -- Force Protection

Air Staff Force Protection

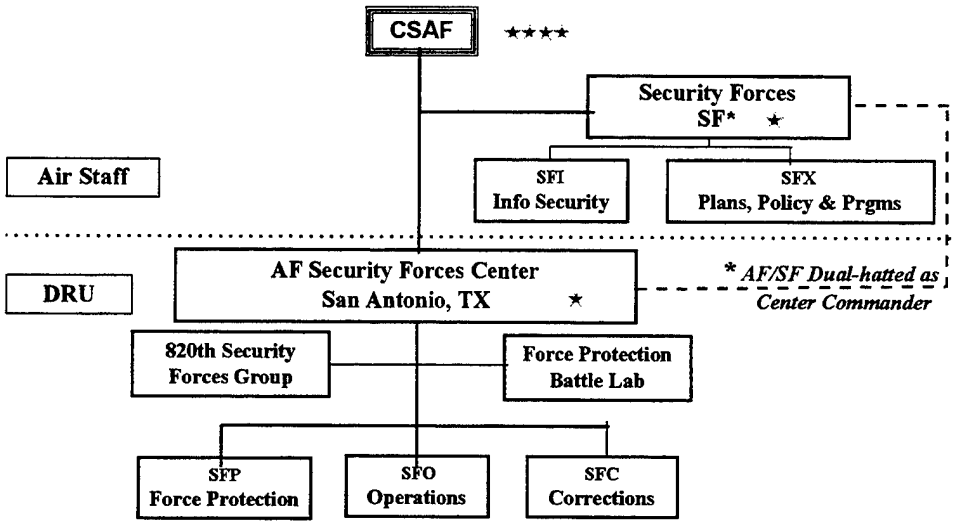


Air Force -- Force Protection



Air Force -- Force Protection

Security Forces Organization



Air Force -- Force Protection

820th SECURITY FORCES GROUP

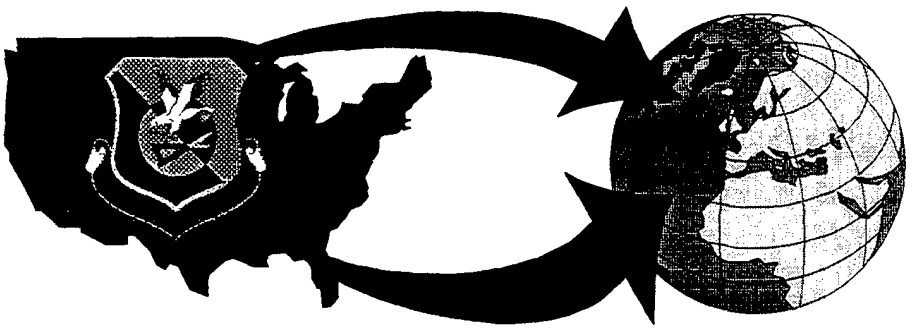
Air Force -- Force Protection

820th Security Forces Group

- CSAF directed organization
- Commander -- Colonel
- Stood-up on 17 Mar 97
- Initial operational capability NLT 1 Jul 97
- Full operational capability NLT 1 Oct 97

Air Force -- Force Protection

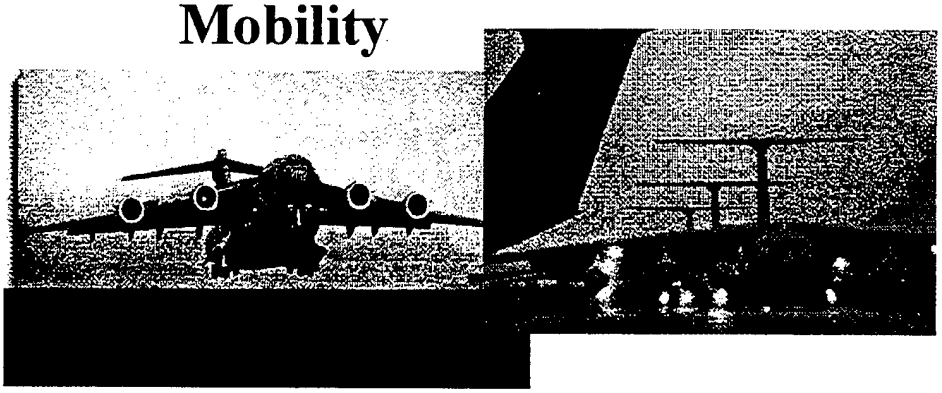
820 SFG Concept of Operation



Cohesive, multi-disciplined, force capable of rapid deployment and ready to employ measures necessary to ensure optimum protection of Air Force resources and personnel

Air Force -- Force Protection

Rapid Mobility

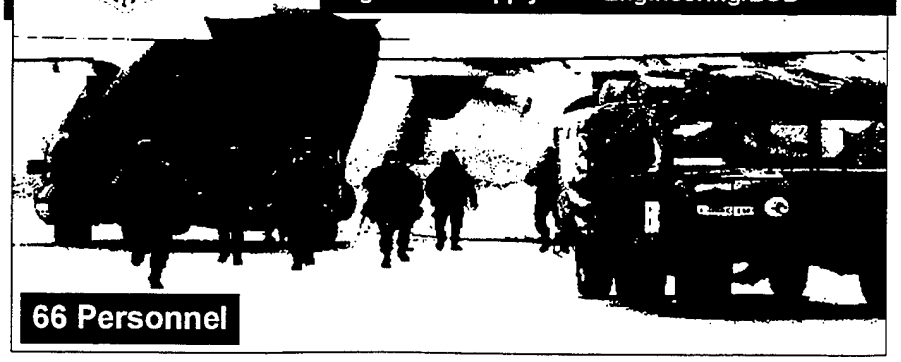


- **Core Unit**
  - **Roll-on -- Roll-off (w/vehicles)**
  - **Palletized (w/prepositioned vehicles)**

Air Force -- Force Protection

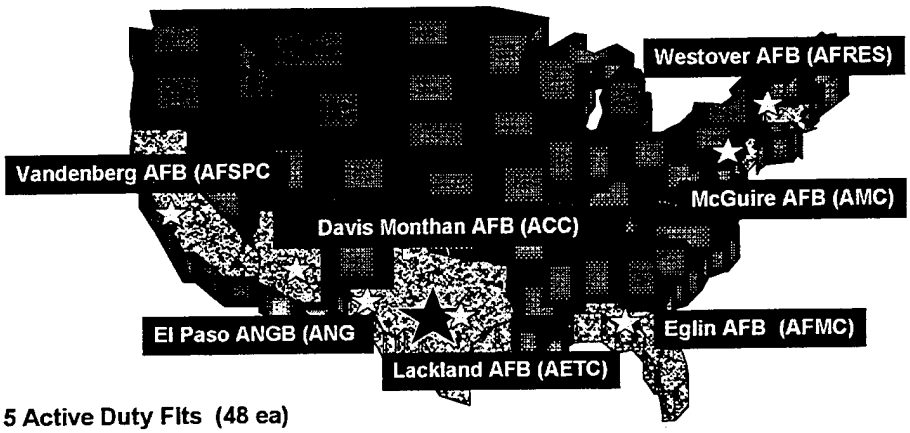
820 SFG HQs Composition

Commander	Air Transportation
Security Forces	Vehicle Maintenance
OSI	Medical
Intelligence	First Sergeant
Communications	Personnel & Admin
Logistics & Supply	Engineering/EOD



Air Force -- Force Protection

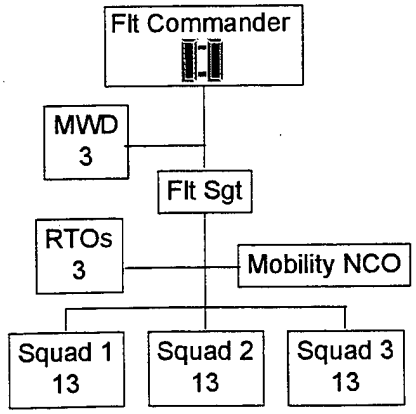
Security Forces Flight Locations



5 Active Duty Flts (48 ea)
1 AFRES Flt (45)
1 ANG Flt (Heavy Weapons) (86)

Air Force -- Force Protection

Security Forces Flight



Air Force -- Force Protection

820 SFG Training Requirements

- Officer Training
  - ABD Level IV (Basic Officers Course)
  - ABD Command Course (Field Grade Officer)
  - Intel Course (Fort Huachuca -- S2)
  - EOD Senior Officer Course (Indian Head MD -- S3)
  - Disaster Preparedness Senior Officer Course (Ft McClellan AL)

Air Force -- Force Protection

820 SFG Training Requirements

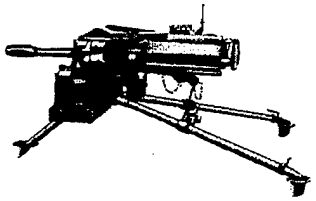
- NCO Training
  - ABD Level II (NCO Course)
  - ABD Command Course (SNCOs)
  - Intelligence Course (Ft Huachuca)

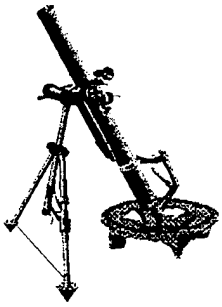
820 SFG Specialized Training

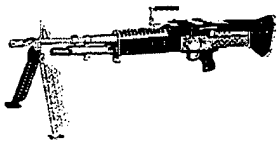
- Based on SFG/CC determination
  - Dynamics of International Terrorism
  - U.S. Army Ranger School
  - Air Assault School
  - Latin American Orientation Course
  - Middle East Orientation Course
  - Infantry Mortars Leaders Course (IMLC)
  - CE Readiness Refresher Course
  - AC-130 Call for Fire Course
  - Federal Post-Blast Analysis Course
  - Chem/Bio Course

820th Security Forces Group Weapons

M - 60	(7.62)	M - 9	(9mm)
Mk 19	(40mm)	M - 2	(50 cal)
M - 16	(5.56)	M - 29	(81mm)
M - 249	(5.56)(SAW)		



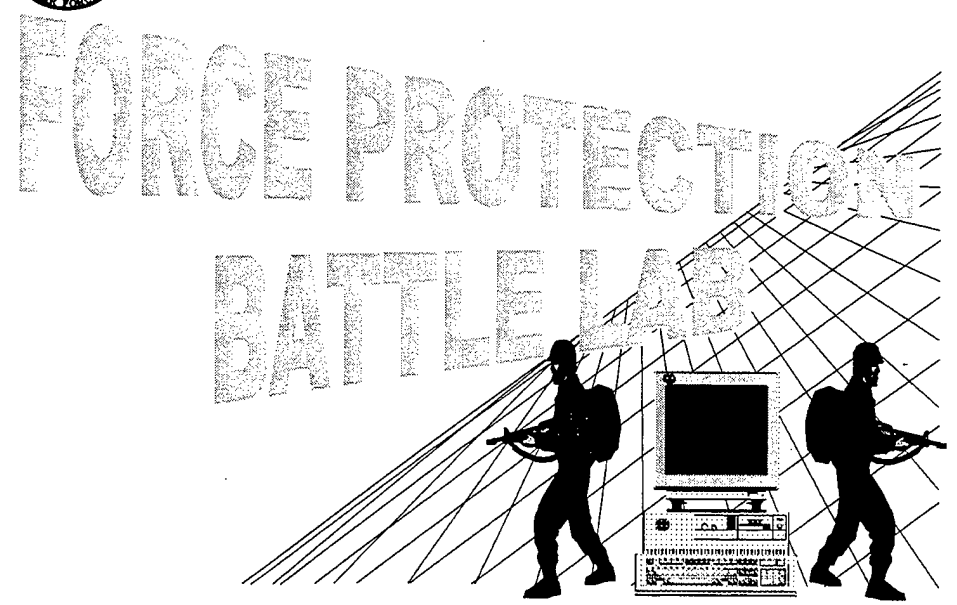




Equipage

- Relocatable Sensor System
- Tactical Automated Sensor System
- Under Vehicle Surveillance Systems
- Thermal Imagers
- Surveillance systems
- Up-armored HMMVWs
- Body armor
- Weapons (lethal/Nonlethal)
- Communications

Air Force -- Force Protection



Force Protection Battle Lab

- New organization focused on exploring and integrating technology, tactics and training to increase force protection readiness
- Cross functional unit manned by SF, OSI, IN, CE, Explosive Ordnance Disposal (EOD), SC and other specialties, as required
- Added to AF Battle Lab Task Force -- one of six labs
- Organization stood-up on 1 Apr 97
- Initial operational capability NLT 1 Jul 97
- Full operational capability NLT 1 Oct 97

Charter

Exploit existing/conceptual technology

- Optimize tactical sensor systems
- Innovative application of COTS systems
- Complement MWD capability with emerging explosive detection technology
- Integrate Chem/Bio detection systems
- Apply UAV potential to force protection

Air Force -- Force Protection

Airpower sized to mission --

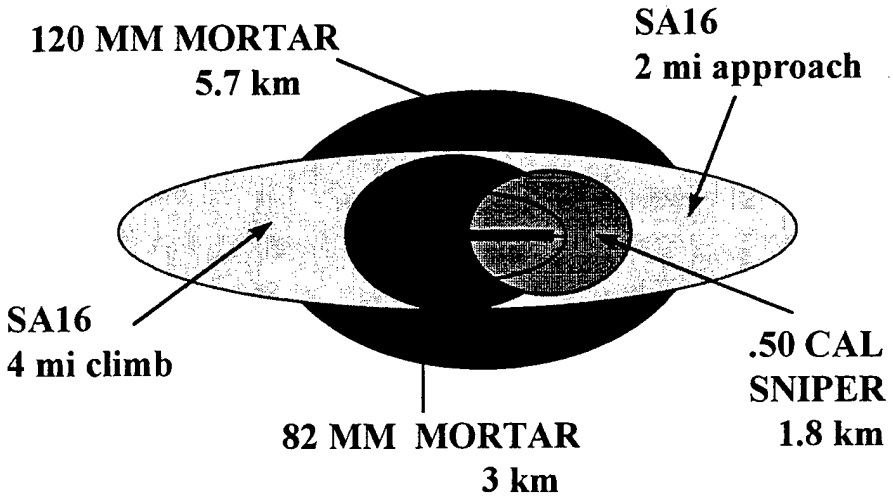
Air Force -- Force Protection

Threats

- **LEVEL I -- Small scale operations conducted by agents, sympathizers, partisans, and terrorist groups.**
-
- **LEVEL II -- Includes long range reconnaissance, intel gathering, and sabotage operations conducted by special purpose forces, guerrilla forces, unconventional forces, or small tactical units.**
- **LEVEL III -- Airborne, heliborne, or amphibious attack through major attacks by aircraft and theater missiles armed with conventional or NBC weapons**

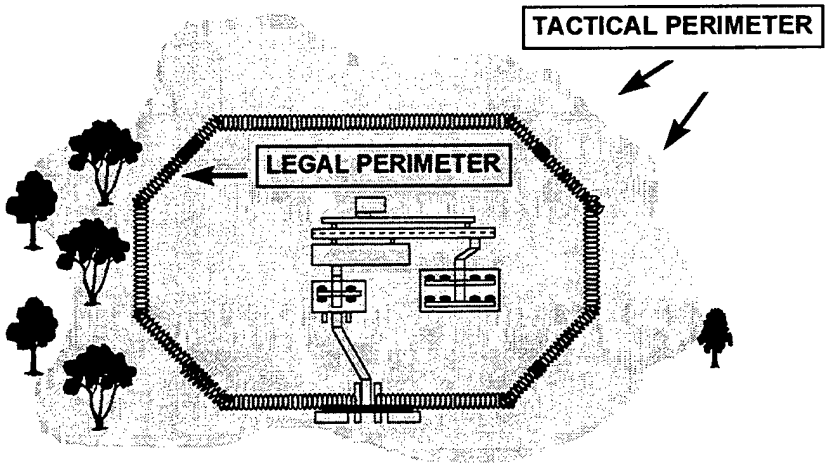
Air Force -- Force Protection

Stand-off Threat



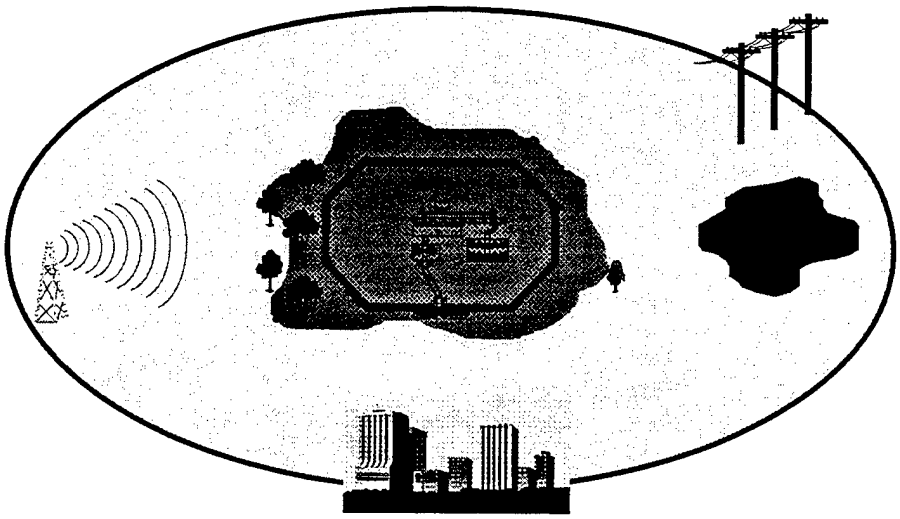
Air Force -- Force Protection

Areas of Responsibility



Air Force -- Force Protection

Area of Interest



Air Force -- Force Protection

Air Force Actions

- **Overview**
  - **DoD and Air Force Guidance**
  - **Force Protection Operations**
  - **Personnel**
  - **Physical Security**
  - **Equipage**
  - **Intelligence**
  - **Training**
  - **Related Studies**

DoD and Air Force Guidance

- New Joint "Commander's Handbook for Antiterrorism Readiness"
- DoD 2000.12 "DoD Combating Terrorism Program
- DoD O-2000.12-H "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence"
- DoD 2000.14 "DoD Combating Terrorism Program Procedures"
- DoD 2000.XX "DoD Combating Terrorism Standards" (DRAFT)
- AFI 31-210 "The Air Force Antiterrorism Program"

Force Protection Operations

OSI

- Conducts
  - Force Protection Briefing Program
  - Vulnerability Assessments
- Integrates with 820 SFG Intel (S-2) and Ops (S-3)
  - S-2 provides tactical intelligence support and connectivity to national level OSI strategic intelligence support and other intel sources
  - S-3 provides linkage with AST and integrates OSI into SFG planning

Force Protection Operations

OSI

- **Antiterrorism Specialty Team (AST)**
  - **Repository of expertise; Rapid Response AT/Force Protection (FP) Capability, basic 6 man element**
  - **Deploys with SFG and chops to deployed unit/CC**
  - **Conduct vulnerability surveys, countersurveillance and high-risk protective service operations**
  - **Establish source networks and collect intelligence on terrorist threat**

Air Force -- Force Protection

Force Protection Operations

OSI

- **Ongoing 24-hour countersurveillance operation at Al Kharj**
- **Expanded photographic and video surveillance theater-wide**
- **Increased Protective Services Operations (body guard)**
- **Increased protection measures for convoy routes**

Air Force -- Force Protection

Personnel

- SF manpower requirements increased from 450 to 1,118 theater wide--presently 892 SPs in-theater
  - Military working dog teams increased from 35 to 44--presently 36
  - OSI manpower increased from 15 to 25 theater wide
- Additional 12-mo PCS billets ID'd (JTF SWA/4404th)
  - CENTCOM reviewing
  - Security Police leadership positions at major installations
  - 1 key Intelligence J-2 position
  - 7 OSI positions

Air Force -- Force Protection

Personnel

- 18 OSI positions and Joint Intelligence Chief (JIC) changed from 90 - to 179 day rotations
- CENTCOM reviewing tour lengths

Air Force -- Force Protection

Physical Security

- **Rapidly relocated forces in Saudi Arabia from dense urban areas to less vulnerable locations**
  - **Operation DESERT FOCUS relocation plan initiated 3 Aug and completed 30 Sep 96**
    - **Provides wider perimeters, improved surveillance and detection opportunity, and allows more robust protective measures**
    - **Approximately 3600 people relocated while operations continued**

Air Force -- Force Protection

Physical Security
Construction Requirements

- **Prince Sultan AB, Al Kharj, Saudi Arabia**
  - **Installed fences and barricades**
  - **Constructed berms**
    - **Bermed billeting, power plant, and fuel bladders**
  - **Construct modular facilities -- Spring '98**
    - **Statement of Work complete, negotiations with Ministry of Defense and Aviation (MODA) on going**

Physical Security

Construction Requirements

- Eskan Village, Saudi Arabia
  - Created 400' exclusion zone, north side
  - Constructed entry control points & barriers
  - Installed Mylar windows
  - Create 1200' stand-off area -- TBD
    - Negotiations with MODA are underway for formal acquisition of additional property
  - Construct blast wall
    - KSA to fund at $1.3M, concept approved

Air Force -- Force Protection

Equipage

- AF accelerated deployment of equipment
  - 19 Hand Held Thermal Imagers
    - 168 additional on order
  - 16 Vehicle Mounted Thermal Imagers
    - $500K additional funding ~ 50 units
  - 6 Low Light Video Recorders
- Mini Intrusion Detection System--9 sets deployed
- Added 152 night vision goggles
- Six remote viewing kits for hand held thermal imagers
- 20 Under Vehicle Surveillance System sets funded at $800K

Air Force -- Force Protection

Equipage

- 900 M-16A2s
- $47M accelerated for Tactical Automated Security System (TASS)
  - Contract let 28 Oct 96
  - CENTCOM Prioritized List
    - Al Jabber Mar 97
    - Eskan Apr 97
    - Ali Al Saleem May 97
    - Al Kharj Jun 97
    - SWA AOR Full Operational Capability - Oct 97

Air Force -- Force Protection

Intelligence

- Commander JTF- SWA created Force Protection Fusion Cell (IN, OSI, SF) at Eskan Village
  - Gathers all source data, processes data, and provides theater specific analysis
  - Ensures timely, analyzed information is provided to wing CC, wing intel, and shared with SF/OSI

Air Force -- Force Protection

Intelligence

- Intelligence will augment deploying SF units, when appropriate, to serve as liaison for intelligence crossflow
- AF/IN actively working with DCI to speed promulgation of guidelines for sanitization and release of intelligence
- DIA to extend Defense Intelligence Threat Data System to Air Force and Navy counterintelligence organizations in FY 97 (funded)
  - Prototype to be fielded Mar 97 with HQ AFOSI
  - Field units to receive operational version Spring 97

Air Force -- Force Protection

Training

- Level 1: Individual Awareness
  - Annual AT Awareness Training
  - Mandatory orientation at new duty station
  - Long-term
    - Basic Military Training
    - Officer accession programs
    - Professional Military Education
    - NCO Promotion Fitness Examination

Air Force -- Force Protection

Training

- **Level 2: Unit level**
- **Unit AT/FP Officer/NCO**
- **Security Police developed course of instruction for all AF/FP representatives**
  - **Award Special Experience Identifier**
  - **AT expert to deploy forward**

Air Force -- Force Protection

Training

- **Level 3: Commanders**
  - **AT Training in MAJCOM Sq/CC Orientation Seminar**

Air Force -- Force Protection

Training

- Level 4: Senior/executive Leadership
  - Selected O-6 through O-8
    - Installation commanders and JTF/Battle Group commanders
  - National Defense University Seminar

Air Force -- Force Protection

Training

- Surgeon General
  - Self Aid/Buddy Care Training
    - Include CPR training for all AF personnel
    - Unit Monitors trained: ECD Jun 97
    - Initial and Annual CPR training for AF personnel: ECD Jun 98
  - Establish IPT for review of AF medical policies, directives and programs
    - Co-chaired by XO/SG
    - Emphasize redirection of focus to preventive medical measures

Air Force -- Force Protection

Training

- Surgeon General
  - Enhance Mass Casualty Training: ECD 1 Aug 98
    - Expand Advance Trauma Life Support Training
      - Include medical providers on identified critical mobility positions
    - Integrate non-medical support personnel into planning and exercise activities
    - Emphasize BW/CW medical response/procedures during casualty scenarios
    - Evaluate Medical Automation Administration Systems for patient tracking information

Air Force -- Force Protection

AFSAA Force Protection Study

- Initiated by AF/XO
  - Members: CE, IN, SF, XO, OSI
  - Completion Date: Apr 97
- Determine the current environment and context affecting USAF force protection
  - Identify major threats to AF force protection
  - Define goals and requirements necessary for AF to address each threat (Concentrate initially on the terrorist threat)
- Investigate historical and innovative alternatives for enhancing force protection

Air Force -- Force Protection

Rand Research Effort

- New Study: Terrorism and Counterterrorism: Implementation for Strategy and USAF Planning
- Key Tasks:
  - Support current Air Staff efforts to address terrorism
  - Explore trends in the nature of terrorism
  - Assess national and global vulnerabilities relative to USAF operations
  - Examine the role of air and space power in counterterrorism
  - Identify implications for US and USAF strategy and planning

Air Force -- Force Protection

Summary

- AF addressing Force Protection issues across a wide front
- Deployed forces are better protected, less vulnerable-- Improvements continue
- Reorganizing to maintain proper institutional focus on FP
- Funding issues are identified, receiving higher priority
- Changing the AF "culture" toward FP
- Active in DoD efforts to protect all personnel
- Must anticipate and protect against ever changing threat

Air Force -- Force Protection

We cannot become confused about the fundamental purpose of our armed forces. That purpose is their readiness to fight and win our nation's wars. As we reshape and train our forces, it must be for this purpose above all others

U.S. MARINE CORPS FORCE PROTECTION PROGRAM OVERVIEW

DEFENSE SCIENCE BOARD TASK FORCE

22 APRIL 1997

AGENDA

- USMC APPROACH TO FORCE PROTECTION
- FORCE PROTECTION PROGRAM ELEMENTS
  - DOCTRINAL/REGULATORY GUIDANCE
  - TRAINING AND EDUCATION
  - SECURITY ASSESSMENTS
  - SECURITY ENHANCEMENTS
- COMMANDER'S RESPONSIBILITIES

USMC APPROACH

- FORCE PROTECTION IS AN OVERARCHING CONCEPT FOCUSED ON MEASURES THAT:
  - PROTECT MARINES, THEIR FAMILIES, AND OUR CIVILIAN EMPLOYEES FROM THREATS TO THEIR PERSONAL SECURITY
  - PROTECT OUR EQUIPMENT AND FACILITIES
- SIMPLY PUT, FORCE PROTECTION IS TAKING CARE OF OUR PEOPLE AND RESOURCES.

DOCTRINE AND REGULATORY GUIDANCE

- FMFM 7-14 (COMBATING TERRORISM) PROVIDES COMMANDER GUIDANCE
  - PROJECTED FOR INTRODUCTION INTO THE MARINE CORPS DOCTRINAL PUBLICATION (MCDP) SERIES UPON NEXT REVISION
- FMFRP 7-14A (INDIVIDUAL'S GUIDE TO UNDERSTANDING AND SURVIVING TERRORISM) PROVIDES INDIVIDUAL AWARENESS INFORMATION
  - JS GUIDE 5260 MIRRORS FMFRP 7-14A

DOCTRINE AND REGULATORY GUIDANCE

- MCO 3302.1B (ANTITERRORISM PROGRAM)
  - REQUIRES UNIT LEVEL ANTITERRORISM OFFICER
  - PRESCRIBES CONDUCT OF ANNUAL TERRORISM RESPONSE EXERCISE AND ANNUAL AT TRAINING
  - OUTLINES MEASURES TO BE TAKEN UNDER VARIOUS TERRORIST THREAT CONDITIONS

- OPNAVINST 5530.14B (DON PHYSICAL SECURITY & LOSS PREVENTION MANUAL)
  - UNIFORM SECURITY STANDARDS FOR DON ACTIVITIES
  - PLANNED REVISION WILL INCORPORATE THE 32 STANDARDS IDENTIFIED BY DOD/J34

FORCE PROTECTION TRAINING AND EDUCATION

- "EVERY MARINE A RIFLEMAN" CONCEPT SUPPORTS FORCE PROTECTION EFFORT

- SPECIALIZED TRAINING FOR SELECTED CATEGORIES OF PERSONNEL
  - AT INSTRUCTOR QUALIFICATION COURSE
  - COMBATING TERRORISM ON MILITARY INSTALLATIONS
  - DYNAMICS OF INTERNATIONAL TERRORISM
  - CONVENTIONAL PHYSICAL SECURITY

FORCE PROTECTION TRAINING AND EDUCATION

- MCO 3302.1B REQUIRES ANNUAL TRAINING FOR ALL HANDS
- TERRORISM AWARENESS FOR ENLISTED MARINES INCLUDED IN ANNUAL MARINE BATTLE SKILLS TRAINING
- MARINE CORPS INSTITUTE COURSE 02.10b "TERRORISM AWARENESS FOR MARINES" (REVISED AUG 96)

FORCE PROTECTION TRAINING AND EDUCATION

- IMPLEMENTED TRAINING TO MEET CJCS REQUIREMENT TO PROVIDE FP/AT TRAINING TO ALL DEPLOYING PERSONNEL
- 4-LEVELS OF TRAINING
  - LEVEL I: INDIVIDUAL AWARENESS TAUGHT BY UNIT FP/ATOFFICERS USING SERVICE POI
  - LEVEL II: UNIT FP/AT OFFICER TRAINING CONDUCTED BY MTTs AND FORMAL SCHOOLS
  - LEVEL III: COMMANDERS TRAINING PROVIDED AS CORE SUBJECT IN COMMANDER'S COURSE
  - LEVEL IV: EXECUTIVE TRAINING TAUGHT AT NDU

SUMMATION OF FORCE PROTECTION TRAINING REQUIREMENTS

- ALL HANDS: ANNUAL TRAINING
- DEPLOYING PERSONNEL: LEVEL I WITHIN 6 MONTHS OF DEPLOYMENT
- UNIT AT/FP OFFICERS: LEVEL II UPON ASSIGNMENT OF FP/AT DUTIES
- CO CERTIFIES TO GAINING CINC THAT ALL HAVE RECEIVED REQUIRED TRAINING

SECURITY ASSESSMENTS

- VULNERABILITY ASSESSMENTS: LOOK FROM BOTH SIDES OF THE FENCE.
  - SYSTEMS APPROACH: PHYSICAL SECURITY, ACCESS CONTROL, THREAT WARNINGS AND INDICATORS, EMERGENCY REACTION PLANS.
  - A TOTAL LOOK AT THE PHYSICAL SECURITY OF FACILITIES, OPERATING PROCEDURES, ADEQUACY OF RESOURCES, AND ABILITY TO IMPLEMENT MEASURES FOR HIGHER THREAT CONDITIONS (THREATCONS) AS SET FORTH IN MCO 3302.1B

WHO DOES THE ASSESSMENT?

- CI/NCIS: THREAT ASSESSMENT AND WARNING DISSEMINATION (AS REQUIRED)
- PMO: PHYSICAL SECURITY EVALUATION OF KEY FACILITIES, I.E., ARMORIES, CPs, ETC. (ANNUALLY)
- TECH REPS: ENGINEERS FROM CONTRACTED NAVAL SUPPORT ACTIVITIES (EVERY 3 YEARS)

WHO DOES THE ASSESSMENT?

- IGMC: PHYS SECURITY/ANTITERRORISM INCORPORATED AS SPECIAL INTEREST ITEM AND INSPECTED IN CONCERT WITH IGMC REVIEW OF COMMAND INSPECTION PROGRAM (UNANNOUNCED, SHORT NOTICE)
- DEFENSE SPECIAL WEAPONS AGENCY (AS REQUESTED)
  - MCAS IWAKUNI, JAPAN
  - MCAS FUTENMA, OKINAWA

SECURITY ENHANCEMENTS

- DEDICATED PHYSICAL SECURITY PROGRAM PROVIDES FUNDING TO AID COMMANDERS IN COMPLYING WITH SECURITY STANDARDS
  - FY97: $6.0 MIL
  - FY98 & 99: $3.8 MIL
  - FY00 - 03: $7.0 MIL
- PBD 098/098c ALLOCATED FUNDS TO
  - STAFF 2 CIVILIAN ANALYSTS AT HQMC FOR FORCE PROTECTION PROGRAM MANAGEMENT
  - FUND MOBILE TRAINING TEAMS TO SUPPORT COMMAND TRAINING AND ASSESSMENTS

SECURITY ENHANCEMENTS

- EMBRACE TECHNOLOGY WHERE FEASIBLE
  - INTRUSION DETECTION SYSTEMS
  - AUTOMATED ENTRY CONTROL SYSTEMS
- OPERATING FORCES HAVE FORMED FP ASSESSMENT TEAMS TO SUPPORT DEPLOYED UNITS
  - MEF CI PERSONNEL AND NCIS CONDUCTING SITE ASSESSMENTS FOR DEPLOYED UNITS
  - CID WARRANT OFFICER ADDED TO MEU COMMAND ELEMENT TO PROVIDE SECURITY ASSET AND ASSIST MEU CI OFFICER

SECURITY ENHANCEMENTS

- PARTICIPATING IN DOD/JCS FORUMS WHICH WILL ENHANCE FP EFFORT
  - JOINT WARFIGHTING CAPABILITY ASSESSMENT (JWCA) ON COMBATING TERRORISM
  - ANTITERRORISM COORDINATING COMMITTEE (ATCC) AND ATCC SENIOR STEERING GROUP
  - PHYS SECURITY EQUIPMENT ACTION GROUP (PSEAG))
  - JOINT SECURITY CHIEFS COUNCIL (JSCC)
  - PHYSICAL SECURITY REVIEW BOARD (PSRB)

- FORMED HQMC FP WORKING GROUP IN SEP 96 TO ADDRESS FP ISSUES

SECURITY ENHANCEMENTS

- ACTIVATED CHEMICAL-BIOLOGICAL INCIDENT RESPONSE FORCE (CBIRF) THAT PROVIDES CAPABILITY TO RESPOND TO CHEM-BIO TERRORIST THREATS

- DEDICATED SECURITY ASSETS ENHANCE FORCE PROTECTION CAPABILITIES
  - MILITARY POLICE
  - EXPLOSIVE DETECTION DOGS
  - ORGANIC UNIT COUNTERINTELLIGENCE
  - MCSF/FAST

COMMANDER'S RESPONSIBLITIES

- CHANGE THE MINDSET FROM REACTIVE TO PROACTIVE; INSTILL FORCE PROTECTION AS A PART OF DAILY BUSINESS.
- BE FAMILIAR WITH THE REFERENCES AND USE DUTY EXPERTS TO SUPPORT EFFORT.
- ENSURE MARINES RECEIVE REQUIRED TRAINING.

COMMANDER'S RESPONSIBLITIES

- INCORPORATE TERRORIST SCENARIOS INTO UNIT LEVEL EXERCISES.
- CAPITALIZE ON ALL-SOURCE INTELLIGENCE.
- ENSURE SOPs, OPERATION PLANS AND DEPLOYMENT ORDERS ADDRESS FORCE PROTECTION CONSIDERATIONS.

COMMANDER'S RESPONSIBLITIES

- DEVELOP A UNIT SECURITY PLAN.
- IDENTIFY REQUIREMENTS AND BUDGET FUNDS TO SUPPORT PROGRAM NEEDS.

USMC OBJECTIVES

- CAPITALIZE ON EXISTING FOUNDATION PUT IN PLACE AFTER THE BEIRUT BOMBING.
- INSTITUTIONALIZE FORCE PROTECTION IN THE WAY WE DO BUSINESS -- TAKING CARE OF OUR MARINES.
- FORCE PROTECTION IS A LEADERSHIP RESPONSIBILITY INHERENT TO COMMAND.