STRATEGY RESEARCH PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

DOMESTIC MILITARY INSTALLATION FORCE PROTECTION: SETTING THE CONDITIONS FOR SUCCESS

BY

LIEUTENANT COLONEL WALTER N. FOUNTAIN
United States Army

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

20020604 196

USAWC STRATEGY RESEARCH PROJECT

Domestic Military Installation Force Protection: Setting the Conditions for Success

by

Lieutenant Colonel Walter N. Fountain
United States Army

Colonel Richard H. Gribling
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

ABSTRACT

AUTHOR: Lieutenant Colonel Walter N. Fountain

TITLE: Domestic Military Installation Force Protection: Setting the Conditions for Success

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 44 CLASSIFICATION: Unclassified

This paper considers how to best resource force protection activities at domestic military installations. The paper considers and expands upon the following discussion points:

– The terrorist attack on U.S. soil on 11 September 2001 has greatly changed the paradigm of force protection operations at domestic military installations.

– The funding for installation antiterrorism programs competes with other installation funding requirements and flow primarily through the Military Services.

– Antiterrorism funding within the Defense Department was decidedly weighted to counter threats at installations and activities outside the U.S.

– Commanders often misinterpret the Posse Comitatus Act of 1878 impeding the coordination and synchronization of force protection activities.

The paper recommends the following:

– DoD policy should require quarterly vulnerability assessments by the local commander on all military installations within the U.S. and require annual oversight of all installation vulnerability assessments by the higher headquarters regardless of size.

– DoD should undertake a comprehensive study of its counterintelligence and law enforcement agencies to identify "best practices" and also should adjust current policy allowing DoD intelligence personnel to provide dedicated analytical support to force protection.

– DoD policy should include a required standard for the conduct of criticality assessment on all military installations. Policy should also address a new standard for Military Service Chiefs and CINCs to conduct criticality prioritization amongst all military installations under their authority and responsibility.

– DoD policy should direct commanders to resource all personnel requirements to enable implementation of FPCON BRAVO without routine augmentation from non-security force tenant units. SECDEF should request relief from 10 U.S.C. 2465, Contracting for Performance of Civilian Commercial or Industrial-type Functions.

TABLE OF CONTENTS

ABSTRACT ..... **III**

LIST OF ILLUSTRATIONS ..... **VII**

DOMESTIC MILITARY INSTALLATION FORCE PROTECTION: SETTING THE CONDITIONS FOR SUCCESS **1**

HISTORICAL BACKGROUND **2**

LACK OF REQUIRED FUNDING 2

LOW-THREAT ENVIRONMENT 2

THE POSSE COMITATUS ACT 3

CONTROL AND OVERSIGHT OF MILITARY INTELLIGENCE ACTIVITIES 4

CURRENT POLICY **5**

U.S. ARMY 10

Recommendations for the U.S. Army **12**

U.S. MARINE CORPS 12

Recommendations for the U.S. Marine Corps **14**

U.S. NAVY 14

Recommendations for the U.S. Navy **16**

U.S. AIR FORCE 17

Recommendations for the U.S. Air Force **18**

RECOMMENDED ACTIONS **19**

ASSESS INSTALLATION VULNERABILITIES 19

CREATE MORE EFFECTIVE LINKAGE BETWEEN INTELLIGENCE AND COMMANDERS 20

PRIORITIZE REQUIREMENTS BY MISSION CRITICALITY 22

ESTABLISH A SECURITY FORCE 23

CONCLUSION **25**

ENDNOTES **27**

BIBLIOGRAPHY 33

LIST OF ILLUSTRATIONS

FIGURE 1. WORLDWIDE DEPARTMENT OF DEFENSE ANTITERRORISM FUNDING ALLOCATION – FISCAL YEAR 1999 THROUGH 2001 (DOLLARS IN BILLIONS) 6

FIGURE 2. DOD ANTITERRORISM PROGRAM CONCEPT 7

FIGURE 3. ANTITERRORISM PROGRAM FUNCTIONS FOR INSTALLATION COMMANDERS 9

FIGURE 4. U.S. NAVY REGION/SHORE STATION FORCE PROTECTION STRATEGY 15

DOMESTIC MILITARY INSTALLATION FORCE PROTECTION: SETTING THE CONDITIONS FOR SUCCESS

> We will direct every resource at our command – every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence, and every necessary weapon of war – to the destruction and to the defeat of the global terror network.
>
> —President George W. Bush, September 20, 2001[1]

The heinous attacks of September 11, 2001 on the World Trade Center complex and the Pentagon must be a catalyst to review current Department of Defense (DoD) policy guidance and resourcing for the conduct of force protection activities on all domestic military installations. For years, military installations outside the United States had actively pursued force protection operations to secure personnel and property from the threat of terrorist attacks. Organizations such as the Bader-Meinhoff Gang and the Red Brigades were examples of host-nation domestic terrorist groups, which actively targeted and attacked US military operations in Europe. In the opinion of General Montgomery Meigs, Commanding General of U.S. Army Europe and Seventh Army, the "game has changed." During the last few decades of the 20th century, "the threat was the politically inspired terrorist with limited objectives," according to Meigs. However, "now we have a kind of messianic and suicidal" terrorist who threatens not only military installations and units, but now "it's [the] people in our whole communities that are targets."[2] This new dynamic in terrorist method of operations as well as the unexpected success of terrorist attack on U.S. soil demonstrated on September 11th, has greatly changed the paradigm of force protection operations at domestic military installations. It is within this new threat environment that U.S. military force protection operations must be reevaluated. In the words of General Meigs, we must generate "mental discipline and creativity that matches what the other guy is doing."[3]

The U.S. military leadership can set the conditions for success in the protection of domestic military installations by instituting and resourcing these four steps:

- Comprehensively assess installation vulnerabilities;
- Create more effective linkage between intelligence agencies and commanders who must allocate resources;
- Prioritize resource requirements by mission criticality;
- Establish a security force presence that does not depend collaterally upon military personnel.

HISTORICAL BACKGROUND

Four major issues have deeply affected the DoD's leadership thinking regarding force protection activities within the United States – a lack of funding; consensus view of a low-threat environment; the Posse Comitatus Act of 1878; and, the control and oversight of all U.S. intelligence activities involving U.S. persons.

LACK OF REQUIRED FUNDING

The funding for installation antiterrorism programs competes with other installation funding requirements. The Congressional Budget Office estimates the amount necessary to sustain U.S. military forces operation and maintenance requirements at current level is under-funded at least $5 billion per year.[4] The CBO's estimate of a sustaining budget estimates the budgetary resources required to sustain today's operations and maintenance activity at their current size and level of activity. Therefore, it could be extrapolated to be conservative since the attacks of 11 September 2001 have greatly increased the level of antiterrorism activity. The General Accounting Office sampled 11 of the 835 military installations in the U.S. and found them to have received only about 22 percent of the funding they requested for antiterrorism initiatives.[5]

In 1996, the Secretary of Defense established the Combating Terrorism Readiness Initiatives Fund. The fund's purpose is to provide unified combatant commanders with funding for unanticipated antiterrorism requirements resulting from changes in the terrorist threat level or service force protection guidance. In FY2000, the entire $15 million in the fund was provided for overseas operational requirements.[6] This fund, although a laudatory attempt to wedge budget resources to react to a fluid threat environment, did nothing to help reduce the effect of the 78% shortfall for funding of domestic installation antiterrorism requirements.

LOW-THREAT ENVIRONMENT

> During the Civil War, a Union General named John Sedgewick stood surveying his Confederate adversary across the battlefield. Confident of his superior position, he turned to an aide and said, "They couldn't hit an elephant at this distance." A moment later, a sharpshooter's bullet struck him under his left eye, killing him instantly. Complacency can kill.
>
> —Donald H. Rumsfeld, U.S. Secretary of Defense, June, 2001[7]

Complacency does kill; however, it may be somewhat unfair to characterize the level of antiterrorism operations at domestic military installations as complacent. Complacency is a feeling of security, while unaware of some potential danger; smug satisfaction with an existing situation.[8] There is little evidence that Defense Department leadership viewed security at

domestic military installations with "smug satisfaction." However, there existed a prevailing feeling of a low-threat environment surrounding military installations within the U.S. In March 2001, Vice Admiral Thomas R. Wilson, Director, Defense Intelligence Agency, and therefore dual-hatted as the U.S. Joint Staff's senior intelligence officer (J2), addressed the greatest threats to the United States interest within the next 12-24 months. He identified a major terrorist attack against United States interests, either here or abroad, as his chief concern. He further identified the terrorists' move toward "higher-casualty attacks" as predictably probable.[9]

An anonymous wit once opined "policy is that which is funded." As noted earlier, antiterrorism funding within the Defense Department was decidedly weighted to counter threats at installations and activities outside the U.S where the threat was widely reported to be at a medium to high level. Most installation commanders rely upon threat estimates developed by the Federal Bureau of Investigation (FBI), or threat estimates developed by military law enforcement agencies, which in turn rely heavily upon the threat predictions of the FBI.[10] FBI reports prior to 11 September 2001 assessed the threat posed by both domestic and foreign terrorist groups within the United States as low. Consequently, during Congressional testimony in June 2001, the Installation Commander of Fort Bragg, NC, the Army's "premier power projection platform," noted terrorism as last in a list of seven probable or potential threats to the installation.[11] Complacency – no, but clearly there was not a high level of concern regarding the security of domestic military installations due to the predicted low-threat environment.

THE POSSE COMITATUS ACT

The Posse Comitatus Act of 1878 (United States Code, Title 18, Section 1385), commonly referred to simply as Posse Comitatus, is often misinterpreted by commanders as an absolute barrier preventing them from undertaking action or coordination involving civilian law enforcement agencies.[12] The Act's intent is to exclude the use of regular military forces (authorized under Title 10, U.S.Code) from conducting domestic police activities. Thus, military officers are concerned with breaking the law by being involved in law enforcement activities, such as force protection activities inherently involving property and space located off the installation. This chilling effect is unwarranted and is often an unnecessary constraint because Posse Comitatus does not necessarily apply in cases of "a sudden and unexpected civil disturbance, disaster, or calamity . . ."[13] The General Accounting Office (GAO) noted this hesitancy of installation commanders to actively engage state, local, and federal law enforcement officials when developing their installation threat assessments.[14] This blinds the

installation commander to a full understanding of the threat, a necessity when attempting to counter the diffuse nature of the current threat to domestic military installations.

CONTROL AND OVERSIGHT OF MILITARY INTELLIGENCE ACTIVITIES

Executive Order (EO) 12333 of December 4, 1981, entitled "United States Intelligence Activities," established the goal, direction, duties, responsibilities, and procedures with respect to and in pursuit of a coordinated, effective national intelligence effort.[15] President Reagan's EO 12333 is the current controlling legal authority regarding the conduct of all U.S. intelligence activities involving U.S. persons. However, EO 12333 was not the first effort within the U.S. Government to correct a perceived ill in the activities of military intelligence units within the domestic arena. It was proceeded by EO 11905 signed by President Ford in 1976 and EO 12036 signed by President Carter in 1978. These actions by the Executive Branch were in reaction to Congressional investigations and hearings conducted in the early 1970s into allegations of military intelligence units' intrusive domestic collection activities.[16]

From the military's point of view, this began quite logically. During the Vietnam War, demonstrations against American involvement in Southeast Asia were assessed to be beyond the ability of civilian authorities to control. Therefore, DoD appointed the Army as executive agent for military assistance to civilian law enforcement authorities. In light of the potential for violent actions to disrupt unit deployments, deploying units requested threat information from the Federal Bureau of Investigation (FBI). However, when the FBI failed to provide the information the Army thought it needed, it began to collect it itself and then shared the information with the FBI and other law enforcement agencies in the spirit of providing military assistance to civilian law enforcement authorities.[17]

The military intelligence personnel proved to be resourceful in their efforts to collect information against potential demonstrators. They intercepted radio communications, conducted surveillance of known demonstrators, and even infiltrated the 1968 Democratic National Convention under media cover. The Congressional investigations into this situation concluded DoD domestic collection efforts had had a chilling effect on Americans who were legally working for political change. Congress likewise realized it had lapsed in its own oversight of the U.S. intelligence community and created the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence in order to provide diligent oversight of intelligence activities.[18]

The executive orders released under the Ford, Carter, and Reagan administrations grew out of the desire to place significant controls on all U.S. intelligence activities involving U.S.

persons. On September 11, 2001, the threat to US internal security assumed a very different face. As details of the breadth and width of this intelligence failure are discovered, it is notable that several of the alleged perpetrators lived within the US for reportedly over one year prior to the attacks.[19] Although it would be more than a little presumptuous to allege the controls placed upon military intelligence collectors caused this egregious "intelligence failure," the idea of information sharing between the domestic law enforcement community and the normally foreign-focused military community now seems a more acceptable risk.

Of interest are the historical "ills" addressed by the EO and Congressional interest revolve around the issue of military intelligence collection infringing on civil liberties. However, current DoD policy takes the concern a step or two further and clearly directs military intelligence personnel to stay more than arms length from any involvement with information concerning U.S. persons or force protection operations within the U.S. It is this attitude of barring even the perception of military involvement in law enforcement activities which has given prudent commanders cause to error on the side of conservatism when interfacing with external agencies regarding the force protection activities of their installations.

CURRENT POLICY

Force Protection has always been a critical mission for the Department of Defense. However, recent terrorist attacks against military activities and forces at home and abroad have brought a renewed, focused effort to improve the military's antiterrorism posture. The Defense Department provides guidance and direction to these activities within DoD Directive 2000.12 entitled "DoD Combating Terrorism Program," and DoD Instruction O-2000.16 entitled "DoD Combating Terrorism Program Standards." Force protection and antiterrorism training programs and requirements are outlined in the companion publication, DoD Directive O-2000.12-H entitled "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence."

DoD policy establishes an antiterrorism force protection program, which is all encompassing program using an integrated systems approach. The program must integrate existing systems within the military services such as physical security, operations security, intelligence, counterintelligence, and chemical and biological warfare.[20] Resources to implement this policy flow primarily through the Military Services. The Chairman of the Joint Chiefs of Staff annually assesses the adequacy of the resources provided by the Services to determine whether they meet DoD AT/FP objectives and support the Unified Commanders AT/FP programs.[21]

DoD has committed significant resources to antiterrorism programs. From fiscal year (FY) 1999 through FY 2001, DoD has spent approximately $10 billion on antiterrorism efforts worldwide. Over 75 percent of this funding went to costs associated with security forces, technicians, and law enforcement.[22] Figure 1 shows the breakout of this funding.

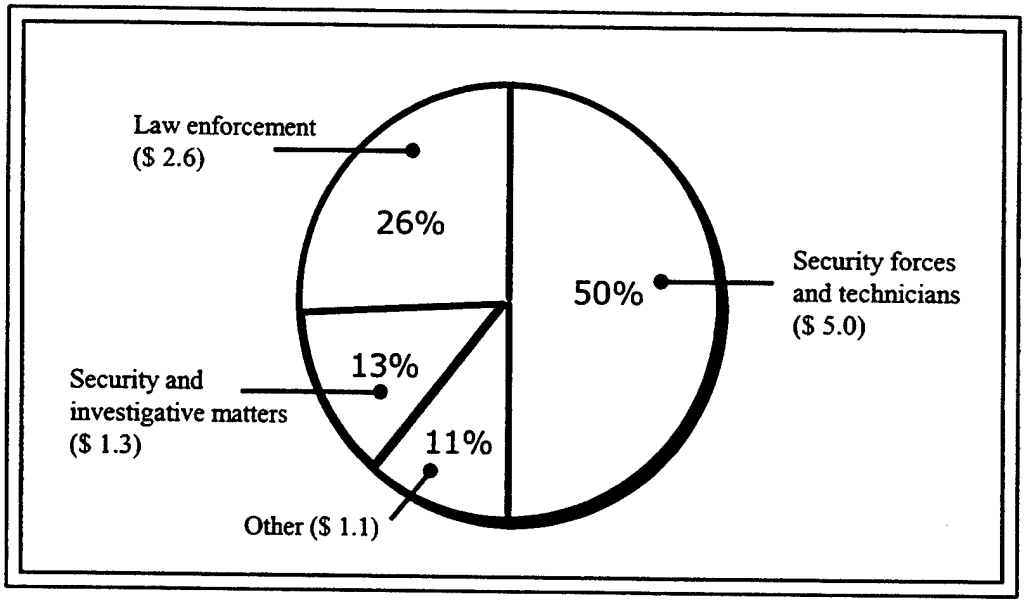

FIGURE 1. WORLDWIDE DEPARTMENT OF DEFENSE ANTITERRORISM FUNDING ALLOCATION – FISCAL YEAR 1999 THROUGH 2001 (DOLLARS IN BILLIONS)[23]

Following the Khobar Towers bombing on 25 June 1996, which killed 19 Air Force personnel and injured hundreds more in Saudi Arabia[24], the Defense Department took decisive action to improve its ability to conduct antiterrorism operations. In October 1996, the Chairman of the Joint Chiefs of Staff established the Deputy Director for Operations for Combating Terrorism (J-34). J-34 has the mission to "support the Chairman and the Joint Chiefs of Staff in meeting the Nation's security challenges as they relate to combating terrorism, now an into the next century."[25] J-34 coordinates and synchronizes the Joint Staff and military services' efforts to conduct efficient and effective antiterrorism and force protection operations. J-34 has published joint antiterrorism doctrine in Joint Publication 3-07.2 entitled "Joint Tactics, Techniques, and Procedures for Antiterrorism."

DoD policy establishes an antiterrorism program concept which has two phases; proactive and reactive. The proactive phase includes the planning, coordinating, resourcing and training required to prevent a terrorist event from occurring. The reactive phase involves the crisis management actions taken to resolve a terrorist event. The concept identifies six steps for the commander to undertake. Step 1 is to determine the terrorist threat to an installation or unit. Step 2 is to assess the vulnerability of unit, installation, base, facility, material, or personnel to

the terrorist threat in order to uncover and isolate security weakness. The third step is to apply operations security measures, personal security measures, physical security measures, and awareness education training in order to mitigate the threat. The fourth step is to understand who has the authority and responsibility to respond to the terrorist threat or action. The fifth step is the establishment of an effective crisis management mechanism in order to respond to a terrorist incident. The last step is to institute a series of graduate measures to counter the terrorist threat as it increases. These threat or force protection conditions have prescribed actions in DoD Directive 2000.12.[26] This antiterrorism program concept is diagramed at figure 2.

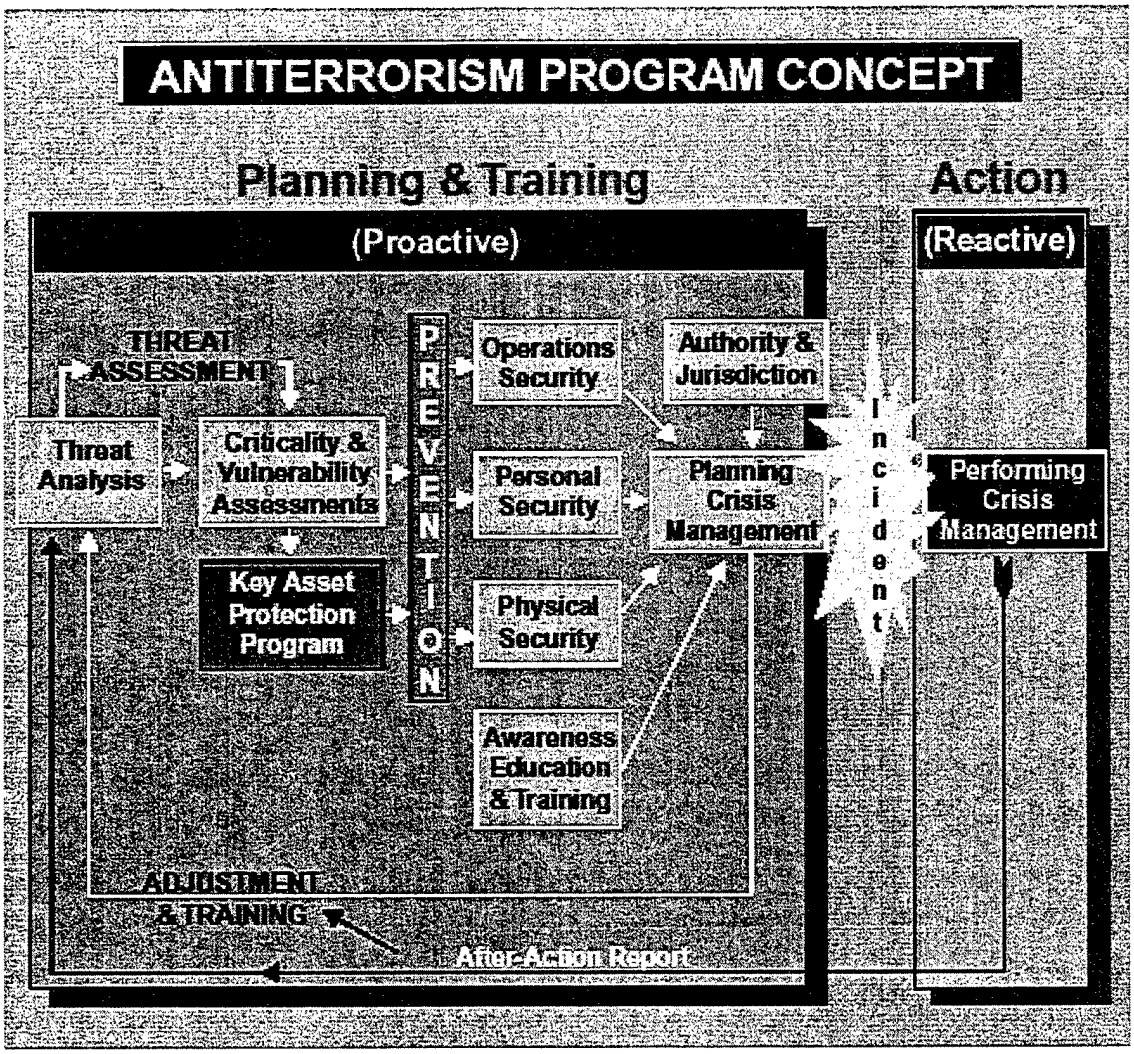

FIGURE 2. DOD ANTITERRORISM PROGRAM CONCEPT[27]

Key to this policy is the requirement of a higher headquarters review of the installation's antiterrorism vulnerability assessment every 3 years. However, current DoD standards require this review only at installations containing more than 300 assigned personnel. This definition reduces the number of domestic installations from 835 to 247. Without this liberalization of the requirement, the Military Services completed higher headquarters assessments at only 30 percent of domestic installations from 1997 through 2000.[28] As a direct result, J-34, in addition to drafting, publishing, and updating antiterrorism standards and policies, conducts independent vulnerability assessments to assist installation commanders in meeting their force protection responsibilities.

The Joint Staff has six assessment teams to conduct vulnerability assessments at both overseas and domestic installations. The assessment teams are called Joint Service Integrated Vulnerability Assessment (JSIVA) teams. These teams conduct assessments on 90 – 100 worldwide military installations per year. The team uses DoD antiterrorism standards articulated within DoD Instruction 2000.16 as the basis for these assessments. The following key elements are addressed: terrorism threat assessment, physical security measures, terrorist incident response measures, and consequence management measures.[29] This directly evaluates the DoD antiterrorism program functions at each installation as shown in Figure 3.

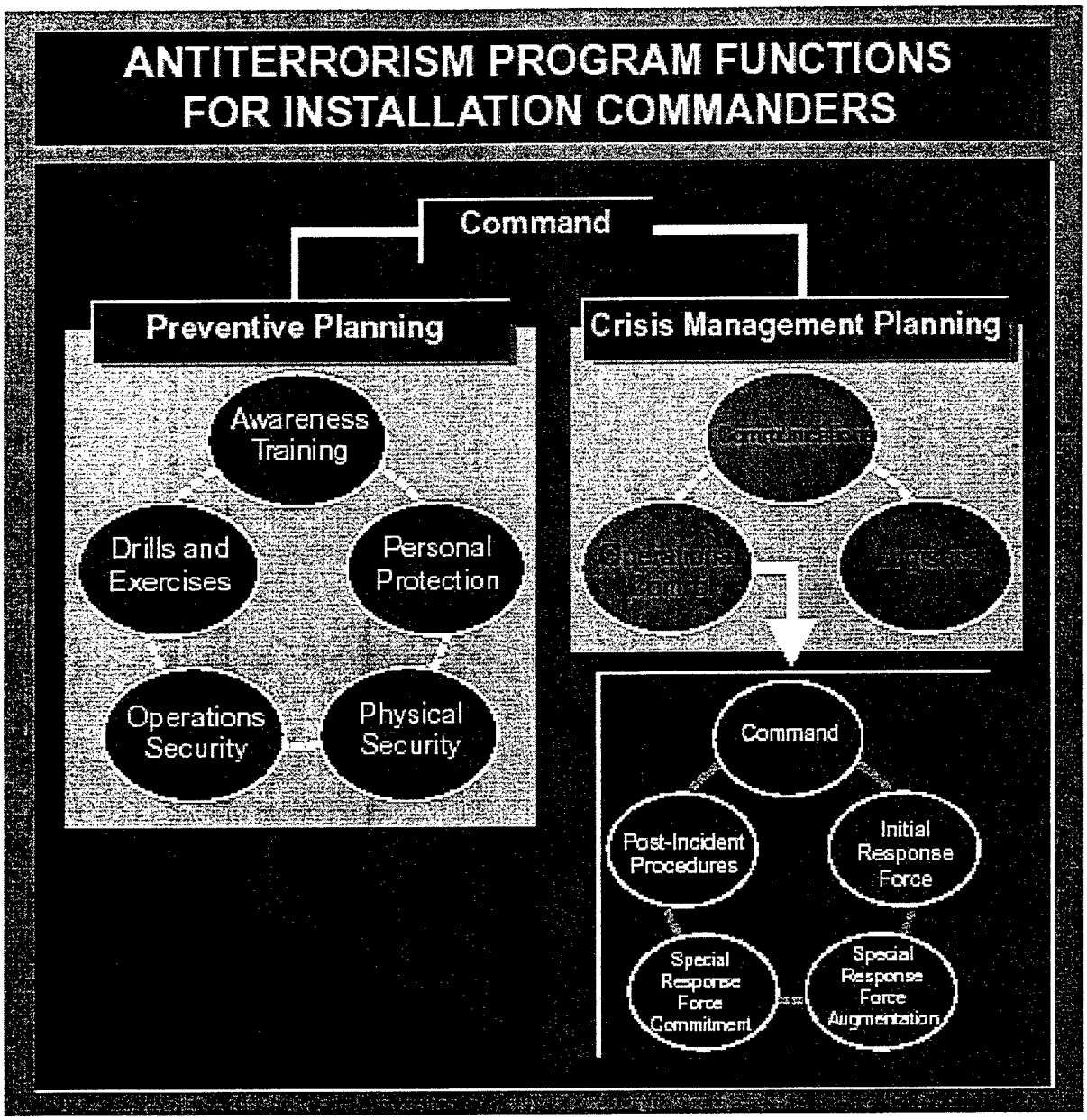

FIGURE 3. ANTITERRORISM PROGRAM FUNCTIONS FOR INSTALLATION COMMANDERS[30]

Through DODI 2000.16, DoD Antiterrorism Standards, and "lessons learned" from the JSIVA visits to the installations, J-34 has significant influence upon the antiterrorism and force protection programs within the military services. This influence is directly exercised in DOD Antiterrorism Coordinating Committee (ATCC). The ATCC is co-chaired by the J-34 and Assistant Secretary for Defense/Special Operations-Low Intensity Conflict (ASD/SO-LIC).[31] Each Service is also represented on the committee. The following subsections discuss the

antiterrorism and force protection program execution of each military service who are directly responsible for antiterrorism/force protection activities at all Service installations within the United States.

U.S. ARMY

The base policy for the Army Antiterrorism and Force Protection program is outlined in Army Regulation (AR) 525-13, Antiterrorism Force Protection (AT/FP): Security of Personnel, Information, and Critical Resources. The latest version is dated 10 September 1998. The regulation implements DoD Directive 2000.12 and DoD Instruction O-2000.16 by providing guidance and mandatory standards for protection Department of the Army personnel (soldiers, civilian employees, and family members), information, and critical resources.[32]

AR 525-13 identifies the U.S. Army's antiterrorism force protection policy as consisting of two tenets: prevent threat incidents though implementation of appropriate protective and preventive measures; and, respond quickly and efficiently when a threat attack is detected. The Army policy is designed to synchronize existing security programs to ensure that antiterrorism force protection is conducted with maximum efficiency. The key elements to the holistic program are: physical security, command and control (C2) protect (maintaining effective command and control of friendly forces while negating or turning to friendly advantage the adversary's efforts to influence, degrade, or destroy friendly command and control systems), personal security, law enforcement, and operations security.[33]

Army policy requires each installation commander to conduct a vulnerability assessment of his or her installation every three years. Additionally, higher headquarters will conduct a similar assessment of installations under their oversight every three years. The assessments verify the installations compliance with all applicable Army and DoD standards. A JSIVA visit meets these requirements.[34] Commanders must also exercise their antiterrorism force protection plan annually. These assessments and exercises are the basis under which commanders justify requests for antiterrorism force protection funding.

Recognizing the potential for significant operational conflicts and resource shortfalls, the Army directs commanders to assess and control these risks when establishing, exercising, and executing their antiterrorism force protection plans. Integrated risk management in the planning, coordinating, and development of antiterrorism force protection plans and ensure that the implementation cost of additional antiterrorism measures does not outweigh the potential benefits.[35]

Until September 2001, most U.S. Army installations within the United States were open installations with unrestricted vehicle access to the garrison areas. These garrison areas often contain many critical and sensitive sites. As an example, Fort Bragg, North Carolina, had three State highways transit the installation. Fort Bragg was not unique in exposing these vulnerabilities to criminal activity and terrorist actions, however, arguably, Fort Bragg may be one of the most high profile terrorist targets. Fort Bragg, a home to the XVIII Airborne Corps, 82d Airborne Division, and the U.S. Army Special Operations Command, must maintain the U.S. Army's premier power projection platform required to launch the Army's first strike capability within 18 hours or less. It is home to almost 10 percent of the U.S. Army's active component forces and provides support services to more than 250,000 soldiers, civilian employees, family members and retirees.[36]

In early 2001, the U.S Army issued orders that required installations to establish a vehicle registration program and commence control measures at the major access points in order to reduce the likelihood of criminal or terrorist threat activity. Additionally, installations must maintain random vehicle checks on secondary access points. However, the Army did not provide funding required to implement the order. Using Fort Bragg again as an example, the directed level of access control required a minimum of 225 Military Policemen, with a surge requirement for total access control of 555 Military Policemen. If the entire XVIII Airborne Corps Military Police Brigade would be dedicated to this mission, there would still be a daily shortfall of 205 Military Policemen. Most commanders would attempt to alleviate this situation with the use of a contracted guard force. However, 10 U.S.C. 2465, Contracting for Performance of Civilian Commercial or Industrial-type Functions prohibits commanders from contracting guard services unless the contract was in place on September 24, 1983.[37] Therefore, an installation commander's only realistic option is military manpower borrowed from tenant units. This option often becomes most untenable when most needed, as during crisis, many soldiers are involved in deployment or mobilization activities.

The U.S. Army is the only service that maintains separate law enforcement and counterintelligence commands. The Criminal Investigation Command (CID) and the Intelligence and Security Command (INSCOM) do not have a command and control relationship. However, their detachments routinely support the installation commanders at domestic military installations. As mentioned earlier, many commanders have a "hands-off" philosophy in regards to intelligence regarding their installations when it is provided by military organizations. It then follows that commanders will rely more heavily on law enforcement information. This was demonstrated in recent Congressional testimony when an Army installation commander referred

to receipt of intelligence updates, he only mentioned being "tied in" with the Federal Bureau of Investigation.[38]

Recommendations for the U.S. Army

The U.S. Army could greatly improve the effectiveness its force protection and antiterrorism efforts by an intra-service review of the criticality of its installations. Currently, the U.S. Army does not require, and hence did not perform, a higher headquarters assessment of 239 of their domestic military installations. The number of installations deemed to be non-critical may in fact be correct, however, further analysis indicates that these non-assessed installations were not selected by a process identifying them as less critical. The installations not assessed by higher headquarters include 14 ammunition plants and five depots.[39]

The U.S. Army continues to severely constrain its installation commanders by not fully resourcing their reasonable personnel requirements. The example above of the Army's directive to close and man installation access points is a case in point. The concept of controlling access to installations is good, but to not provide funding or manpower in which to institute the policy, is shortsighted at best. In the words of one major Army installation commander, the restricting of access to the installation during increased levels of threat is "very resource intensive" and requires the use of non-security personnel from tenant units. The significant detrimental effect of using these soldiers is the risk to personnel readiness. The soldiers are unable to train on their assigned mission skills when augmenting force protection security forces.[40] The only adequate solution is for the U.S. Army to resource all personnel requirements to enable implementation of FPCON BRAVO without routine augmentation from non-security force tenant units.

The challenge of separate law enforcement and counterintelligence commands is one that the Army must study. Short of combining the commands, greater synergy between the commands and installation-level detachments could be gained through more co-location of elements and exchange of liaison officers between command elements. A focused information campaign to educate commanders on the use of their law enforcement and intelligence personnel in light of current policy might dispel some of the myths concerning the restrictions imposed by Posse Comitatus.

U.S. MARINE CORPS

Marine Corps force protection policy 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 responsible for the security of all personnel within their unit. The Marine

Corps antiterrorism policy is directed in Marine Corps Order (MCO) 3302.1B. The doctrine for Marine Corps antiterrorism force protection operations is found in Fleet Marine Force Manual (FMFM) 7-14, Combating Terrorism. In 1997, the Marine Corps developed a Marine Corps Force Protection Campaign Plan.[41] The Marine Corps, in a General Accounting Office report to the House Armed Service Committee in September 2001, touted this plan as a major antiterrorism initiative.[42]

Due to its administrative tie to the U.S. Navy, the Marine Corps also must follow the specific policy set forth in Operational Navy Instruction (OPNAVINST) 5530.14B, Department of the Navy Physical Security and Loss Prevention Manual. This instruction establishes uniform security standards for the U.S. Navy and Marine Corps activities. U.S. Navy antiterrorism force protection policy will be discussed further in the next subsection.

The operational standards used by the Marine Corps to measure and evaluate installation and unit antiterrorism readiness are the Marine Corps Combat Readiness Evaluation System (MCCRES) Mission Performance Standards. The standards provide training objectives and are integrated with other Marine Corps mission performance standards. The Marine Corps antiterrorism program addresses seven major elements: threat estimate; installation/unit criticality and vulnerability assessments; operations security; personnel security; physical security; crisis management planning; and, employment of tactical measures to contain and counter terrorist incidents.[43]

The Marine Corps centers their antiterrorism force protection program on the concept of an alert, educated, and combat-ready Marine is the best deterrent against terrorism. However, it is not in the training of its Marines that the Marine Corps finds it greatest force protection vulnerabilities. In February 1999, Camp Pendleton, California underwent a JSIVA team evaluation. Camp Pendleton is the major West Coast Marine base. It is home to 60,000 personnel (Marines, Sailors, Soldiers, Airmen, civilian employees, and dependents) who work or live on Camp Pendleton. The JSIVA visit identified several vulnerabilities in the antiterrorism force protection posture of the base. The actions required to mitigate or eliminate these vulnerabilities totaled $3.3 million. However, requests through the Combating Terrorism Readiness Initiative Fund (CBTRIF) only netted $285,000 to meet these unfunded requirements.[44]

As with many of the Military Services, the Marine Corps must contend with large, sprawling installations. Camp Pendleton is one of the largest and geographically complex installation in the United States. It covers 200 square miles in size, has 17 miles of open coastline along its perimeter, and must contend with approximately 62,000 vehicles entering its

gates each and every day. This creates a significant challenge for the commander to resource access control and perimeter protection requirements.[45] Marine Corps leadership clearly understands the drain of military manpower in contending with such un- or under-funded installation force protection requirements. In January 2000, the Marine Corps published its campaign plan for installation management reforms. A major tenet of this plan is to civilianize or outsource functions currently being performed by uniformed Marines with the intent to return as many Marines as possible to the operating forces and their warfighting mission.[46]

The Marine Corps looks to the Naval Criminal Investigative Service (NCIS) to provide force protection intelligence and advice to their installation commanders. NCIS provides law enforcement and counterintelligence expertise to the commanders. The responsibilities of the NCIS line up well with the responsibilities of the FBI. This advantages the dissemination and exchange of information between the two organizations, and in turn, increases the installation commander's confidence in the information and advice received from their NCIS agent.[47]

Recommendations for the U.S. Marine Corps

The Marines have the policy and procedures in place in order to effectively conduct force protection antiterrorism activities at their domestic military installations. However, the success of this policy will depend on their ability to fund the reforms outlined in the U.S. Marine Corps Installations Campaign Plan (ICP). Help from DoD will likely be required in order to adequately resource these initiatives.

The Marine Corps could additionally help itself by assessing the criticality of the areas within their installations. One of the challenges of the sprawling nature of the Marine Corps bases is the manpower required to effectively cordon the perimeter. An internal criticality analysis of each base will likely allow commanders to tighten and shorten that perimeter without significantly increasing the risk to critical activities and locations on the installation.

U.S. NAVY

The U.S. Navy antiterrorism force protection program is outlined in the capstone document, Secretary of the Navy Instruction (SECNAVINST) 3300.2A entitled "Department of the Navy Antiterrorism/Force Protection (AT/FP) Program," dated 21 March 2001. SECNAVINST 3300.2A is further supplemented and focused with SECNAVINST 3300.3 entitled Combating Terrorism Program Standards, dated 7 July 1998.

In 1999, the Chief of Naval Operations (CNO) created the N34 Antiterrorism/Force Protection Division within his operations staff. This was the CNO's investment towards a "world class" force protection program within the Navy. The three keys to this program were seen as:

- Command responsibility;
- Change mindset and perceptions towards force protection;
- Effective and efficient risk management program to support commander's decision making.

The CNO believed improving the antiterrorism force protection program would rest on strengthening three pillars: a focused intelligence and dissemination process for threat warning; a robust physical security program, and aggressive use of security technology and systems to reinforce that program; and, well-trained security forces with close links to local and regional civilian reinforcing capability.[48] Like previously noted for the Marine Corps, the Navy shares the advantage of the integration of law enforcement and counterintelligence within the NCIS, their service investigative command.

The U.S. Navy separates its view of antiterrorism force protection strategy into two areas; region/shore station strategy, and port visit strategy. The region/shore strategy is most germane to this paper. Within this strategy, the Navy acknowledges it must operate within a resource-constrained environment and must coordinate with external agencies to coordinate protection of critical nodes and incident response. It maintains a "defense in depth" approach to force protection activities.[49] A diagram of the strategy is at figure 4.

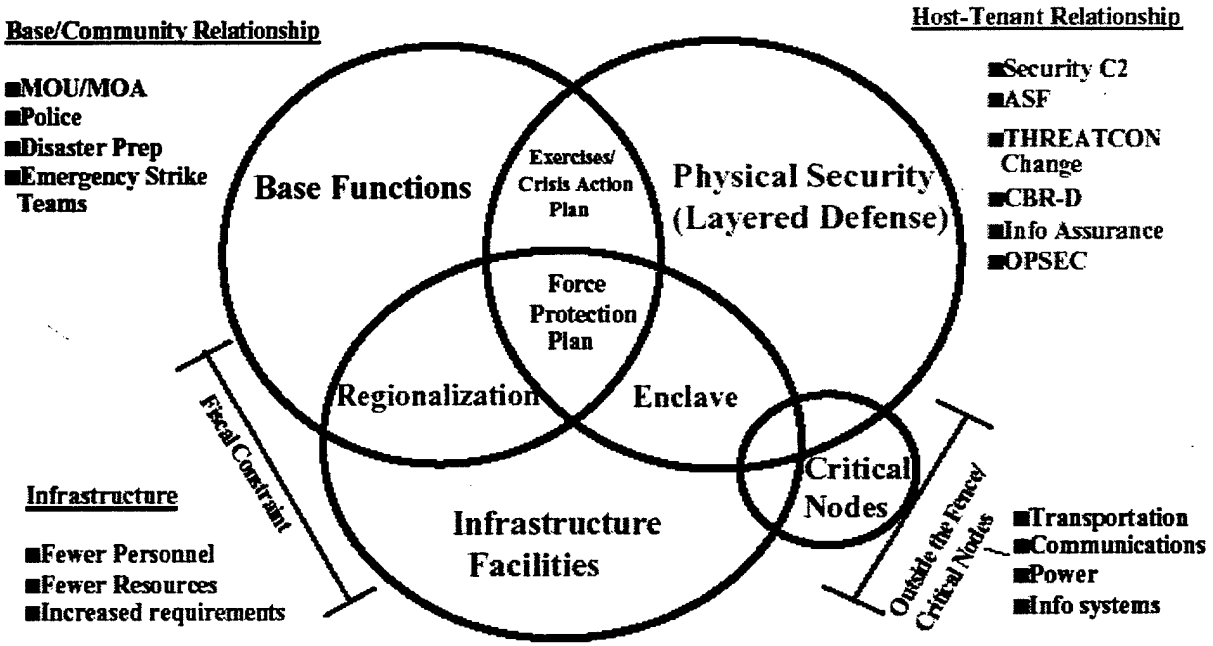

FIGURE 4. U.S. NAVY REGION/SHORE STATION FORCE PROTECTION STRATEGY[50]

The U.S. Navy's "defense in depth" approach to force protection requires commanders to identify Mission Essential Vulnerable Areas. Commanders are expected to provide a second layer of defense for these mission essential areas when the threat condition dictates.[51] This can be a highly effective way to focus the highly constrained resources available for force protection.

The Navy has a similar problem as that pointed out for the Marine Corps in the subsection above. Navy installations are generally sprawling and often have older, failing infrastructure. For example, Naval Station Norfolk, which is homeport for 77 ships and 16 Naval Aviation squadrons with 138 aircraft, has a perimeter that extends over 27 miles. Half of the perimeter is shoreline. The four main vehicular access points do not have securable gates.[52]

Although Naval Station Norfolk faces funding shortfalls as do most military installations, its most severe resource shortfall is in security force manning. The base does not have sufficient military security personnel and civilian police officer to meet all force protection personnel requirements at a normal level of threat condition. Therefore, the base commander must use military personnel augmentees from ships and units in port in order to conduct normal daily antiterrorism force protection operations. The burden upon these warfighting units becomes even more onerous when the threat rises above normal such as the situation military installations have faced since 11 September 2001.[53]

Recommendations for the U.S. Navy

The U.S. Navy's "defense in depth" approach to force protection requires commanders to provide a second layer of defense for their mission essential areas when the threat condition dictates. Most Navy commanders do not have sufficient military security personnel and civilian police officers to meet all force protection personnel requirements at a normal level of threat condition. The force protection security personnel manning situation within the U.S. Navy was the worst reported among senior military installation commanders from all services during recent Congressional testimony.[54] The final solution clearly lies in additional resourcing for this key element of the CNO's strategy, however, the critical interim step has already been identified within the CNO's strategy. The U.S. Navy must undergo a mindset change that force protection is a core competency without which no ship will successfully put to sea. This mindset change must be implemented within the performance evaluation system, education system, and command policies of the U.S. Navy.

In order to ensure scarce and valuable resources are properly directed, the U.S. Navy, like the U.S. Army, should conduct an intra-service review of the criticality of its installations.

Without this formal review, critical installations may receive less priority and fewer resources just based upon their smaller size or population without regard for their criticality to the U.S. Navy's mission accomplishment.

U.S. AIR FORCE

The U.S. Air Force (USAF) antiterrorism force protection program operates under the guidance and policy established in Air Force Instruction (AFI) 31-210 entitled The Air Force Antiterrorism Program, dated 1 August 1999. The instruction implements all applicable DoD directives and instructions. The USAF program rests on five elements: 1) collecting and disseminating timely threat information; 2) training for all USAF members; 3) comprehensive planning to deter, counter, and recover from terrorist incidents; 4) allocating necessary funds and personnel to the conduct of the program; and 5) implementing effective defensive measures. USAF policy acknowledges that antiterrorism/force protection is a command responsibility that must be fully integrated into each and every USAF unit's mission.[55]

The USAF antiterrorism force protection program recognizes the requirement for a fully integrated and coordinated effort is required to effectively counter the terrorist threat. The USAF concept integrates several key functional areas including: civil engineering, communications, intelligence, operations, security forces, medical, legal, and investigative agencies and units.[56]

This integrated approach is also visible in the Air Force Office of Special Investigations (AFOSI) wherein law enforcement and counterintelligence functions are integrated within the same major command. Like the U.S. Navy's NCIS, AFOSI provides installation commanders "one-stop shopping" for information, advice, and assistance in regards to installation force protection issues.

USAF policy requires higher commands to evaluate the subordinate's antiterrorism/force protection program and conduct an assessment of the unit/installation's vulnerability to the terrorist threat. All USAF commanders must conduct a physical security vulnerability assessment at least every three years. These multi-functional teams should address the full spectrum of threats to mission essential critical assets, utilities, facilities, food, and water. The Air Force also established independent Vulnerability Assessment Teams (VAT) that conduct "over the shoulder" observations of the higher commands' assessments.[57]

One could conclude that the USAF has maintained the most vigilant antiterrorism force protection posture of any of the Services over the past decade. Whereas all of the other services instituted open access to their facilities, the USAF has always maintained access control measures at their installations and bases. Although USAF bases are often sprawling

geographically like those mentioned for the USMC and Navy previously, the USAF has invested the resources to completely surround all their bases with physical barriers. For example, Travis Air Force Base in California, which is home to 60th Air Mobility Wing and provides services to more than 25,000 active duty airmen, civilian employees, and dependents, occupies 7,000 acres. In spite of its size, the base has 48 miles of internal security fencing providing redundant intrusion deterrence to the primary physical barrier that protects the entire base perimeter.[58]

The USAF's domestic installations may benefit from an increased physical security infrastructure due to the Service's doctrinal reliance on domestic bases to project its wartime mission. They also benefit from a personnel structure that has been resourced to allow the Air Force to establish similar bases in foreign countries during expeditionary operations. The Air Force has not had to establish these bases in recent years, therefore, it has also not had to adjust for the potential loss of security personnel at domestic bases during these operations.

However, USAF domestic bases have not fared as well as overseas USAF bases in the battle for antiterrorism/force protection resources. One USAF commander attributed this to a better overseas antiterrorism/force protection process that formally defines requirements and establishes priorities. Domestic bases are unable to compete with overseas locations that are combating more recognizable and well-known threats.[59] This lack of a definable, high threat within the U.S. may no longer be applicable since September 11, 2001, but, nonetheless, caught many domestic base and installation commanders without adequate resources to execute necessary antiterrorism/force protection measures.

Recommendations for the U.S. Air Force

Although the U.S. Air Force may be the best postured of all the services to conduct effective force protection antiterrorism operations at their domestic military installations, they are not without weaknesses. A key and critical weakness is their reliance upon the DoD standard that installations without 300 or more personnel assigned do not require periodic assessments by a higher headquarters. This policy has allowed the U.S. Air Force to overlook potentially critical installations such as radar sites, fuel storage facilities, and communications annexes.[60]

Based upon the U.S. Air Force's reliance upon domestic military installations for power projection operations and sanctuary basing for combat missions, a more in-depth review of the criticality of each domestic installation is in order. This intra-service evaluation would ensure proper prioritization of constrained funding and personnel resources. Additionally, it would ensure that force protection protects the capabilities of the U.S. Air Force, not just defend against the purported threat within a geographic location.

RECOMMENDED ACTIONS

The Department of Defense and the Military Services have been doing a good job of preparing domestic military installations against the threat of terrorist attack. The changes that have been made over the past decade, such as JSIVA team visits, instituting vehicular access control at all military installations, and routinely exercising plans to react to various contingencies, are strong, positive examples to argue that DoD is on the right track. However, the nature of terrorism is asymmetric warfare. The terrorists will likely attack where least expected and usually where the target is lightly defended. Therefore, DoD must further expand their antiterrorism force protection efforts to date. Specifically, DoD must take the following actions: comprehensively assess installation vulnerabilities; create more effective linkage between intelligence agencies and commanders who must allocate resources; prioritize resource requirements by mission criticality; and, establish a security force presence, which does not depend collaterally upon military personnel.

ASSESS INSTALLATION VULNERABILITIES

Current DoD policy requires all commanders to prepare a terrorism threat assessment at least annually. This assessment should identify the "full range of known or estimated terrorist capabilities for use in conducting vulnerability assessments and planning countermeasures."[61] The reasoning for this requirement is highly sound. The threat assessment becomes the foundation of all antiterrorism force protection planning, as it is the centering piece for the commander's risk assessment. Within current policy, this importance is recognized. In addition to the annual, comprehensive threat assessment, policy requires the continuous analysis of developing threat information to support the warning process.[62]

However, the policy for threat assessments seems out of congruence with the DoD policy for installation vulnerability assessments. Current policy only requires Unified Commanders (CINCs), Military Service Chiefs, and/or DoD Agency Directors to conduct a Higher Headquarters Vulnerability Assessment once every three years.[63] It is acknowledged that the threat is continually evolving. The bold and audacious nature of the attacks on U.S infrastructure on 11 September 2001 bear clear witness to this fact. This fact, combined with changing infrastructure conditions on and adjacent to installations, improving security technology, and developing "lessons learned' from other installation evaluations, call for a frequent, if not continuous, vulnerability assessment regimen.

The DoD instruction currently requires installation commanders to review their local vulnerability assessment each year.[64] However, it is a common adage that the only things that

get done are those which are checked by someone in authority. As the vulnerability assessment drives the installation's antiterrorism force protection plan, it is crucial for a coherent, timely, and relevant plan to be in step with the near continuous update of the threat situation.

DoD policy for vulnerability assessments is further watered down by the delineation that a "installation" is only a facility that consists of 300 or more personnel on a daily basis.[65] This arbitrary number belies the potential criticality of an installation to the national security of the United States. This focus on avoiding mass casualties has allowed the CINCs and Service Chiefs to ignore a majority of domestic military installations. Therefore, from June 1997 through December 2000, a higher headquarters vulnerability assessment was performed at only 30 percent of the total of 835 domestic military installations.[66]

DoD policy must be amended to account for the current, pervasive threat that terrorists have brought to U.S. soil. DoD policy should require quarterly vulnerability assessments by the local commander on all military installations within the U.S. Additionally, policy should require annual oversight of all installation vulnerability assessments by the higher headquarters regardless of size. It is estimated that DoD would need twelve additional JSIVA teams to extend vulnerability assessment to all domestic installations regardless of size.[67] It could be further interpolated that increasing the frequency to annual vice every three years would require yet another 30 teams. Prioritization of higher headquarters efforts should be directly based upon critically of the installation to nation security, not merely number of personnel assigned.

CREATE MORE EFFECTIVE LINKAGE BETWEEN INTELLIGENCE AND COMMANDERS

Three of the four services within the Department of Defense have consolidated their counterintelligence and law enforcement functions within a single integrated command structure. The U.S. Army stands alone by maintaining these functions separately within the Criminal Investigation Command (CID) and the Intelligence and Security Command (INSCOM), respectively. The potential inefficiencies of this structure within the U.S. Army should be of concern to DoD since the U.S. Army has primary responsibility for force protection antiterrorism activities at nearly half of the domestic military installations.

DoD should undertake a comprehensive study of its counterintelligence and law enforcement organizations. This would be, in effect, an external evaluation of these primarily service functions. The study should endeavor to identify "best practices" within the services' counterintelligence and law enforcement organizations and policies. The conduct of this survey by DoD could break through traditional and parochial views within the services themselves.

Additionally, DoD may recognize efficiencies that could be gained by consolidating certain functions within a joint DoD organization or by appointing a specific service executive agency over specific functions.

Current DoD policy inhibits DoD intelligence personnel, whether active duty military personnel, civilian employees, or contractors, from conducting, or directly assisting in, the time consuming task of synthesizing and analyzing the abundance of law enforcement information and security reports available to the installation commander.[68] DoD should adjust this policy to allow DoD intelligence personnel to provide dedicated analytical support to the force protection effort. Installation force protection working groups have already established liaison with law enforcement and security officials within their regions. One challenge commonly mentioned by installation force protection officers is the overwhelming amount of raw information provided by their regional officials during periods of crisis or heightened security.[69]

Off-installation law enforcement and security officials are genuinely committed to ensuring military installations receive all relevant threat information, but it is generally provided as specific information reports, not as fully analyzed intelligence.[70] Law enforcement agencies are generally reactive analysts as they try to catch and convict criminals. They are too lightly manned, often with no resources at all, to conduct the breadth and scope of predictive analysis conducted routinely by the military intelligence professional. Due to their own resource shortfalls, law enforcement agencies normally provide information to the installation with little or no analysis by the collecting agency. Providing commanders with the trained and dedicated resources to conduct timely, pertinent, and predictive analysis of the voluminous law enforcement and regional threat data which is shared with the installation, gives the commander the means to understand how the information affects his or her force protection posture.

As military intelligence personnel do not initiate any collection activity under this proposed change to policy, the civil liberties of U.S. persons are not jeopardized. This modification in policy does not endorse or anticipate collection tasking authority from the military installation to the civilian law enforcement agency. Therefore, the lawful collection and dissemination of all information provided to the military installation for analysis remains the legal responsibility of the providing agency. Under this proposed change, the critically important objective of providing the best possible force protection for military personnel and facilities is enhanced while maintaining the equally important objective of protecting the Constitutional rights and liberties of all U.S. persons. However, strict guidelines, rigorous oversight (which is already well entrenched), and control of the installation force protection effort by duly sworn law enforcement officials, which at

many installations are federal police, is the most prudent course to allay any fear of military intelligence collection infringing on civil liberties.[71]

In addition to modifying policy to allow DoD intelligence personnel to provide dedicated analytical support to the force protection effort, DoD should seek assistance from the Office of Homeland Security (OHS) to facilitate the horizontal fusion of information. Specifically, OHS has the responsibility to develop a national strategy to secure the United States from terrorist attacks or threats.[72] Therefore, as the OHS develops and promulgates policy to facilitate a seamless intelligence-sharing system, DoD must ensure the effective integration of its installations into this system.

Culturally and technologically, the security and law enforcement communities are not set up to share information at all levels. These obstacles also hinder the efficient exchange of information with domestic military installations. OHS oversees the effort to overcome these impediments. President Bush's 2003 budget submission requested funding to address this issue in many ways. One of the most fruitful may be the requested funding for the FBI to develop a better information architecture to ensure security and law enforcement agencies have instantaneous access to the information they require to effectively combat terrorism.[73] DoD must ensure its domestic military installations are included within this architecture.

In the words of one pundit, "a seamless national intelligence architecture must reach from the streets of New York City to the jungles of Indo-China, and not allow criminals and terrorists to slip between the legal "seams."[74] A simple modification to policy will go a long way to closing one of those 'seams'."

PRIORITIZE REQUIREMENTS BY MISSION CRITICALITY

DoD guidance directs commanders to conduct risk assessment to assist them in making the very real, and often difficult, antiterrorism force protection decisions required in a resource constrained environment. Current policy outlines four elements which must be included within the commander's risk assessment: 1) the terrorist threat; 2) the criticality of the assets; 3) the vulnerability of facilities, programs, and systems to terrorist threat; and 4) the ability to conduct activities to deter terrorist incidents, employ countermeasures, mitigate the effects of a terrorist incident, and recover from a terrorist incident.[75] Asset criticality is noted as a prime input to the commander's ability to establish antiterrorism force protection requirements and properly direct antiterrorism force protection resources.

Unfortunately, DoD policy and guidance does not establish a standard for the conduct of these criticality assessment. The DoD antiterrorism handbook recommends using six factors

(value, materials, significance, accessibility, reconstitution, and mission impact) to assess criticality.[76] Although these are reasonable factors for the commander to consider, they are not required by the directive to be used in the criticality assessment. This lack of specific guidance may be the reason the General Accounting Office found many installation force protection officials did not know how to conduct a criticality assessment. In fact of the eleven domestic military installations visited by the GAO, none had completed a criticality assessment using the six factors identified in the handbook.[77]

In addition to incomplete guidance regarding criticality assessment within military installations, DoD provides no guidance regarding the prioritization of resources based upon the criticality of an installation to national security. This situation is at least partially a result of the military's focus on avoidance of mass casualties, which set the 300 personnel floor for the application of guidance to an installation. As stated earlier, the 300 personnel standard has caused over 70 percent of domestic military installations to be overlooked by higher headquarters vulnerability assessments. For example, these installations included fourteen ammunition plants, seven fuel storage facilities, and three hospitals.[78] Without a higher headquarters vulnerability assessment, it is hard to expect the higher headquarters to have the information and insight into every installation that is required to assess requirements and prioritize resources across several installations. Since 1999, DoD has committed more than $10 billion to improve force protection at domestic installations.[79] However without a prioritization of how critical the installation is to the overall national security objectives, these funds may not have been properly targeted.

The next revision of DoD antiterrorism force protection policy should include a required standard for the conduct of criticality assessment on all military installations. Policy should also be published to address a new standard for Military Service Chiefs and CINCs to conduct criticality prioritization amongst all military installations under their authority and responsibility. These two additions to DoD antiterrorism force protection guidance will greatly improve antiterrorism resource allocation. It should assist in avoiding the current situation wherein a lower priority facility could receive improvements while a more critical facility remains vulnerable to terrorist attack.

ESTABLISH A SECURITY FORCE

In accordance with DoD guidance, the use of security guards is an essential element of a force protection physical security plan. Although recognized as a highly effective part of the

security system, it is also acknowledged as highly expensive.[80] This expense is not only measured in funding outlays but also in manpower and training investments.

Nearly all domestic military installation commanders must rely on augmentation to meet the personnel requirements of their antiterrorism force protection plans. For example, the Commanding Officer of the U.S. Naval Base San Diego, which is home port to almost two-thirds of the U.S. Pacific Fleet, has a manning allowance of 125 civilian and military security personnel. However, as of June of 2001, he only has 97 positions filled, barely three-quarters of the authorization. Further, the Commanding Officer of the U.S. Naval Base Norfolk, which is home port to majority of the U.S. Atlantic Fleet faces similar shortages in his security guard force.[81] Although arguably these two naval installations are the most critical of U.S. Navy bases to U.S. national security, these two major power projection platforms are under-resourced.

Installation commanders faced with personnel shortages in their security forces have only one option. They must try to make up those shortages by pulling personnel augmentees from tenant units or ships. These augmentees have a war-fighting mission not associated with security force duties. This places a two-fold penalty on the commander. First, the augmentees must be trained to standard. This training must be planned and executed by qualified trainers. Secondly, the augmentees are unavailable for training that impacts on their personal and unit readiness. For example, the Installation Commander of Fort Bragg, N.C., routinely draws upon the 82d Airborne Division to fulfill his security force requirements.[82]

DoD policy highlights five force protection conditions (FPCON – formally known as THREATCON) to describe the progressive levels of force protection measure implementation. These conditions range from NORMAL, indicating a routine security posture, to DELTA, indicating a terrorist attack has occurred in the immediate area or intelligence indicates a terrorist attack against a specified target is likely.[83] As discussed above, many critical installations already have difficulty manning their security force at FPCON NORMAL. The standards for required personnel to be on alert or on-site increases commensurate with the increase in FPCON. For a minimum of 90 days after the terrorist attacks of 11 September 2001, all domestic military installations maintained a minimum of FPCON BRAVO.

The force protection measures implemented during FPCON BRAVO must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, or aggravating relations with local community officials.[84] One of the significant measures implemented during FPCOM BRAVO is maintain all personnel involved in implementing antiterrorist contingency plans on two-hour recall to insure readiness. This group of personnel

would include the installation Crisis Management Force and the Special Reaction Team. Based upon the inability of many installations to fulfill personnel requirements at FPCON NORMAL, once installations elevate their FPCON to BRAVO, they must rely heavily on augmented military personnel or units from their tenant organizations. This has a negative impact on the combat mission readiness of these forces.

DoD policy should direct commanders to resource all personnel requirements to enable implementation of FPCON BRAVO without routine augmentation from non-security force tenant units. This commitment of resources would include the manning of all CMF and SRT requirements on a continuous basis with standing forces. This resource investment will allow responsible commanders to meet current published DoD antiterrorism force protection standards without orchestrating a "shell game" of borrowed manpower. It is likely this manpower could only be generated, in the short term, through establishing service contracts for these services. Implementation of these contracts would likely require that commanders receive relief from 10 U.S.C. 2465, Contracting for Performance of Civilian Commercial or Industrial-type Functions, which prohibits commanders from contracting guard services unless the contract was in place on September 24, 1983.[85]

CONCLUSION

Since the heinous and unprecedented attacks of 11th of September 2001 on key economic and political sites within the borders of the United States, it has become necessary for the Department of Defense to reevaluate how it conducts antiterrorism force protection operations at domestic military installations. The attacks were a wake-up call that gave more definition to a threat that was previously characterized as "lower...more predicable...less easy to define."[86] The requirement to improve installation preparedness by assessing their vulnerabilities, creating more effective linkage between intelligence agencies and the commanders who must allocate resources, prioritizing requirements by mission criticality, and establishing a credible security force, which does not completely rely on military augmentees from tenant units, is now clearly proven. The attacks of 11 September 2001 severely disrupted the economic engine of the United States and the global economies. Our national security cannot risk such disruption to our key military power projection platforms in the U.S.

WORD COUNT = 8845

ENDNOTES

[1] President George W. Bush, "Address to a Joint Session of Congress and the American People," September 20, 2001; available from <http://www.whitehouse.gov/news/releases/2001/09/20010920-8.html>; Internet; accessed 9 October 2001.

[2] Erin Q. Winograd, "U.S. Army Europe Chief: Force Protection Needs Demand Mental Agility," Inside the Army, 26 November 2001, 4.

[3] Ibid.

[4] Congressional Budget Office, "Budgeting for Defense: Maintaining Today's Forces," September, 2000; available from <http://www.cbo.gov/showdoc.cfm?index=2398&sequence=3>; Internet; accessed 4 December 2001.

[5] General Accounting Office, Report to the Chairman, Special Oversight Panel on Terrorism, Committee on Armed Services, House of Representatives, "Combating Terrorism: Actions needed to Improve DOD Antiterrorism Program Implementation and Management" (Washington, D.C.: U.S. General Accounting Office, 19 September 2001), 22.

[6] Ibid., 5.

[7] Congress, House, House Armed Services Committee, Prepared Testimony of U.S. Secretary of Defense Donald H. Rumsfeld, 107th Cong., 1st sess., 21 June 2001; available from <http://www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-06-21rumsfeld.html>; Internet; accessed 5 December 2001.

[8] *Random House College Dictionary*, rev. ed. (1980), s.v. "Complacency."

[9] Congress, Senate, Senate Armed Services Committee, Statement for the Record of Vice Admiral Thomas R. Wilson, Director, Defense Intelligence Agency, "Global Threats and Challenges Through 2015," 8 March 2001; available from <http://www.senate.gov/~armed_services/statemnt/2001/010308tw.pdf>; Internet; accessed 5 December 2001.

[10] GAO, 17.

[11] Congress, House, House Armed Services Committee, Special Oversight Panel on Terrorism, Testimony of Col. Addison D. Davis IV, Garrison Commander, 18th Airborne Corps, Ft. Bragg, 107th Cong., 1st sess., 28 June 2001; available from <http://www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-06-28davis.html>; Internet; accessed 6 December 2001.

[12] William H. Harrison, Report to the Honorable Pete Wilson, Governor, State of California: Assessment of the Performance of the California National Guard During the Civil Disturbances in Los Angeles, April and May 1992 [The Harrison Report] (Sacramento, California: State of California, 2 October 1992), 24-25.

[13] Department of the Army, Domestic Support Operations, Army Field Manual 100-19 (Washington, D.C.: U.S. Department of the Army, 1 July 1993), 3-2.

[14] GAO, 5-6.

[15] Executive Office of the President, United States Intelligence Activities, Executive Order 12333 (Washington, D.C.: U.S. Executive Office of the President, 4 December 1981), 2.

[16] U.S. Army Deputy Chief of Staff for Intelligence, "History," a historical summary of intelligence oversight of U.S. Army intelligence activities, n.d.; available from <http://www.dami.army.pentagon.mil/offices/dami-ch/io/faq/history.html>; Internet; accessed 7 October 2001.

[17] Ibid.

[18] Ibid.

[19] Cable News Network, "Experts: A variety of intelligence factors may have played a role," 16 September 2001; available from <http://www.cnn.com/2001/US/09/16/gen.intelligence.terrorism>; Internet; accessed 9 October 2001.

[20] Department of Defense, DoD Antiterrorism/Force Protection (AT/FP) Program, Directive Number 2000.12 (Washington, D.C.: U.S. Department of Defense, 13 April 1999), 3.

[21] Ibid., 11.

[22] GAO, 4.

[23] Ibid.

[24] Lieutenant General James F. Record, USAF, "Independent Review of the Khobar Towers Bombing," 31 October 1996; available from <http://www.af.mil/current/Khobar/recordf.htm>; Internet; accessed 20 November 2001.

[25] Defense Science Board, The Defense Science Board 1997 Summer Study Task Force on DoD Responses to Transnational Threats, Volume II, Force Protection Report (Washington, D.C.: U.S. Defense Science Board, October 1997), 12.

[26] Joint Chiefs of Staff, Joint Tactics, Techniques, and Procedures for Antiterrorism, Joint Publication 3-07.2 (Washington, D.C.: U.S. Department of Defense, 17 March 1998), IV-3-7.

[27] Ibid., IV-2.

[28] GAO, 5-7, 9.

[29] Office of the Secretary of Defense, Report to Congress: Installation First Responder Preparedness (Washington, D.C.: U.S. Department of Defense, 26 March 2001), 6.

[30] Joint Chiefs of Staff, Joint Publication 3-07.2, IV-8.

[31] Joint Chiefs of Staff, Combating Terrorism Readiness Initiatives Fund, Chairman of Joint Chiefs of Staff Instruction 5261.01A, 1 August 1998; available from <http://www.pseag.org/CWG_Documentation/CJCSI%205261-01A.html>; Internet; accessed 9 December 2001.

[32] Department of the Army, Antiterrorism Force Protection (AT/FP): Security of Personnel, Information, and Critical Resources, Army Regulation 525-13 (Washington, D.C.: Department of the Army, 10 September 1998), i-1.

[33] Ibid., 7-8.

[34] Ibid., 11-13.

[35] Ibid., 8.

[36] Congress, House, House Armed Services Committee, Testimony of Col. Addison D. Davis IV.

[37] Ibid.

[38] Congress, House, House Armed Services Committee, Special Oversight Panel on Terrorism, Transcript of Hearing on Security Against Terrorism on U.S. Military Bases, 107th Cong., 1st sess., 28 June 2001; available from <http://commdocs.house.gov/committees/security/has179240.000/has179240_0x.htm>; Internet; accessed 19 December 2001.

[39] GAO, 12.

[40] Congress, House, House Armed Services Committee, Special Oversight Panel on Terrorism, Transcript of Hearing on Security Against Terrorism on U.S. Military Bases.

[41] Defense Science Board, 24.

[42] GAO, 19.

[43] Commandant of the Marine Corps, Combating Terrorism, Fleet Marine Force Manual 7-14 (Washington, D.C.: U.S. Department of the Navy, 5 October 1990), 2-5.

[44] Congress, House, House Armed Services Committee, Special Oversight Panel on Terrorism, Testimony of Major General David F. Bice, Commanding General, Marine Corps Base Camp Pendleton, 107th Cong., 1st sess., 28 June 2001; available from <http://www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-06-28bice.html>; Internet; accessed 6 December 2001.

[45] Ibid.

[46] Commandant of the Marine Corps, Installations Campaign Plan (ICP) (Quantico, VA: U.S. Department of the Navy, 1 January 2000), 20 –21.

[47] Congress, House, House Armed Services Committee, Special Oversight Panel on Terrorism, Transcript of Hearing on Security Against Terrorism on U.S. Military Bases.

[48] Captain Timothy Holden, US Navy, "Force Protection," briefing slides from presentation to the National Defense Industrial Association's 4th Annual Expeditionary Warfare Conference, 1-5 November 1999, Washington, D.C., 3 November 1999; available from <http://www.dtic.mil/ndia/expeditionary/holden.pdf>; Internet; accessed 13 December 2001.

[49] Ibid.

[50] Ibid.

[51] Congress, House, House Armed Services Committee, Special Oversight Panel on Terrorism, Testimony of Captain Joseph F. Bouchard, Commanding Officer, Naval Station Norfolk, 107th Cong., 1st sess., 28 June 2001; available from <http://www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-06-28bouchard.html>; Internet; accessed 6 December 2001.

[52] Ibid.

[53] Ibid.

[54] Congress, House, House Armed Services Committee, Special Oversight Panel on Terrorism, Transcript of Hearing on Security Against Terrorism on U.S. Military Bases.

[55] Department of the Air Force, The Air Force Antiterrorism/Force Protection (AT/FP) Program Standards, Air Force Instruction 31-210 (Washington, D.C.: U.S. Department of the Air Force, 1 August 1999), 2.

[56] Ibid.

[57] Ibid., 9-13.

[58] Congress, House, House Armed Services Committee, Special Oversight Panel on Terrorism, Testimony of Brigadier General Thomas P. Kane, Commander, 60th Air Mobility Wing, 107th Cong., 1st sess., 28 June 2001; available from <http://www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-06-28kane.html>; Internet; accessed 6 December 2001.

[59] Ibid.

[60] GAO, 12.

[61] Department of Defense, DoD Antiterrorism Standards, Instruction Number 2000.16 (Washington, D.C.: U.S. Department of Defense, 14 June 2001), 13.

[62] Ibid.

[63] Ibid., 25.

[64] Ibid.

[65] Ibid.

[66] GAO, 8.

[67] Ibid., 9.

[68] Office of the Secretary of Defense, Policy Guidance for Intelligence Support to Force Protection, SECDEF Message DTG: 181700Z NOV 98, (Washington, D.C.: U.S. Department of Defense, November 18, 1998), 3-9.

[69] Commander, 10th Mountain Division (Light Infantry) and Fort Drum, New York, Force Protection Exercise After Action Report (Fort Drum, NY: U.S. Department of the Army, 15 May 2001).

[70] Ibid.

[71] Admiral James M. Loy and Captain Robert G. Ross, U.S. Coast Guard, "Meeting the Homeland Security Challenge: A Principled Strategy for a Balanced and Practical Response," Journal of Homeland Security, September 2001; available from <http://www.homelandsecurity.org/journal/Articles/Ross_Loy_USCG.htm>; Internet; accessed 20 November 2001.

[72] Executive Office of the President, Establishing the Office of Homeland Security and the Homeland Security Council, Executive Order 13228 (Washington, D.C.: U.S. Executive Office of the President, 8 October 2001), 1.

[73] Tom Ridge, "Remarks to the National Governors' Association Committee on Human Resources," Washington, D.C., 24 February 2002; available from <http://www.whitehouse.gov/news/releases/2002/02/20020224-2.html>; Internet; accessed 2 March 2002.

[74] Robert David Steele, "Possible Presidential Intelligence Initiatives," International Journal of Intelligence and Counterintelligence 13, no. 4(2000): 415.

[75] DoDI 2000.16, 14.

[76] U.S. Department of Defense, Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence, Handbook Number 0-2000.12-H (Washington, D.C.: U.S. Department of Defense, 19 February 1993), 6-13 – 6-14.

[77] GAO, 13.

[78] Ibid., 12.

[79] Ibid., 26.

[80] DoDH 0-2000.12-H, 8-20 – 8-21.

[81] Congress, House, House Armed Services Committee, Special Oversight Panel on Terrorism, Transcript of Hearing on Security Against Terrorism on U.S. Military Bases.

[82] Ibid.

[83] DoDH 0-2000.12-H, BB-1 – BB-7.

[84] Ibid., BB-2.

[85] Congress, House, House Armed Services Committee, Testimony of Col. Addison D. Davis IV.

[86] Congress, House, House Armed Services Committee, Testimony of Brigadier General Thomas P. Kane, Commander, 60th Air Mobility Wing.

BIBLIOGRAPHY

Bush, George W., President of the United States. "Address to a Joint Session of Congress and the American People." September 20, 2001. Available from <http://www.whitehouse.gov/news/releases/2001/09/20010920-8.html>. Internet. Accessed 9 October 2001.

Cable News Network. "Experts: A variety of intelligence factors may have played a role." 16 September 2001. Available from <http://www.cnn.com/2001/US/09/16/gen.intelligence.terrorism>. Internet. Accessed 9 October 2001.

Harrison, William H. Report to the Honorable Pete Wilson, Governor, State of California: Assessment of the Performance of the California National Guard During the Civil Disturbances in Los Angeles, April and May 1992 [The Harrison Report]. Sacramento, California: State of California, 2 October 1992.

Holden, Timothy, Captain, US Navy. "Force Protection." Briefing slides from presentation to the National Defense Industrial Association's 4th Annual Expeditionary Warfare Conference, 1-5 November 1999. Washington, D.C., 3 November 1999. Available from <http://www.dtic.mil/ndia/expeditionary/holden.pdf>. Internet. Accessed 13 December 2001.

Loy, Admiral James M. and Captain Robert G. Ross. U.S. Coast Guard. "Meeting the Homeland Security Challenge: A Principled Strategy for a Balanced and Practical Response." Homeland Security Journal, September 2001. Available from <http://www.homelandsecurity.org/journal/Articles/Ross_Loy_USCG.htm>. Internet. Accessed 20 November 2001.

Record, James F., Lieutenant General, USAF. "Independent Review of the Khobar Towers Bombing." 31 October 1996. Available from <http://www.af.mil/current/Khobar/recordf.htm>. Internet. Accessed 20 November 2001.

Ridge, Tom. "Remarks to the National Governors' Association Committee on Human Resources," Washington, D.C., 24 February 2002. Available from <http://www.whitehouse.gov/news/releases/2002/02/20020224-2.html>. Internet. Accessed 2 March 2002.

Steele, Robert David. "Possible Presidential Intelligence Initiatives." International Journal of Intelligence and Counterintelligence 13, no. 4 (2000): 415.

U.S. Army Deputy Chief of Staff for Intelligence. "History." A historical summary of intelligence oversight of U.S. Army intelligence activities. N.D. Available from <http://www.dami.army.pentagon.mil/offices/dami-ch/io/faq/history.html>. Internet. Accessed 7 October 2001.

U.S. Commandant of the Marine Corps. Combating Terrorism. Fleet Marine Force Manual 7-14. Washington, D.C.: U.S. Department of the Navy, 5 October 1990.

U.S. Commandant of the Marine Corps. Installations Campaign Plan (ICP). Quantico, VA: U.S. Department of the Navy, 1 January 2000.

U.S. Congress, House. House Armed Services Committee. Prepared Testimony of U.S. Secretary of Defense Donald H. Rumsfeld. 107th Cong., 1st sess. 21 June 2001. Available from <http://www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-06-21rumsfeld.html>. Internet. Accessed 5 December 2001.

U.S. Congress, House. House Armed Services Committee. Special Oversight Panel on Terrorism. Testimony of Brigadier General Thomas P. Kane, Commander, 60th Air Mobility Wing. 107th Cong., 1st sess. 28 June 2001. Available from <http://www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-06-28kane.html>. Internet. Accessed 6 December 2001.

U.S. Congress, House. House Armed Services Committee. Special Oversight Panel on Terrorism. Testimony of Captain Joseph F. Bouchard, Commanding Officer, Naval Station Norfolk. 107th Cong., 1st sess. 28 June 2001. Available from <http://www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-06-28bouchard.html>. Internet. Accessed 6 December 2001.

U.S. Congress, House. House Armed Services Committee. Special Oversight Panel on Terrorism. Testimony of Col. Addison D. Davis IV, Garrison Commander, 18th Airborne Corps, Ft. Bragg. 107th Cong., 1st sess. 28 June 2001. Available from <http://www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-06-28davis.html>. Internet. Accessed 6 December 2001.

U.S. Congress, House. House Armed Services Committee. Special Oversight Panel on Terrorism. Testimony of Major General David F. Bice, Commanding General, Marine Corps Base Camp Pendleton. 107th Cong., 1st sess. 28 June 2001. Available from <http://www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-06-28bice.html>. Internet. Accessed 6 December 2001.

U.S. Congress, House. House Armed Services Committee. Special Oversight Panel on Terrorism. Transcript of Hearing on Security Against Terrorism on U.S. Military Bases. 107th Cong., 1st sess. 28 June 2001. Available from <http://commdocs.house.gov/committees/security/has179240.000/has179240_0f.htm>. Internet. Accessed 19 December 2001.

U.S. Congress, Senate. Senate Armed Services Committee. Statement for the Record of Vice Admiral Thomas R. Wilson, Director, Defense Intelligence Agency, "Global Threats and Challenges Through 2015." 8 March 2001. Available from <http://www.senate.gov/~armed_services/statemnt/2001/010308tw.pdf>. Internet. Accessed 5 December 2001.

U.S. Congressional Budget Office. "Budgeting for Defense: Maintaining Today's Forces." September, 2000. Available from <http://www.cbo.gov/showdoc.cfm?index=2398&sequence=3>. Internet. Accessed 4 December 2001.

U.S. Defense Science Board. The Defense Science Board 1997 Summer Study Task Force on DoD Responses to Transnational Threats, Volume II, Force Protection Report. Washington, D.C.: U.S. Defense Science Board, October 1997.

U.S. Department of the Air Force. The Air Force Antiterrorism/Force Protection (AT/FP) Program Standards. Air Force Instruction 31-210. Washington, D.C.: U.S. Department of the Air Force, 1 August 1999.

U.S. Department of the Army. Antiterrorism Force Protection (AT/FP): Security of Personnel, Information, and Critical Resources. Army Regulation 525-13. Washington, D.C.: U.S. Department of the Army, 10 September 1998.

U.S. Department of the Army. Commander, 10th Mountain Division (Light Infantry) and Fort Drum, New York. "Force Protection Exercise After Action Report." Fort Drum, NY: U.S. Department of the Army, 15 May 2001.

U.S. Department of the Army. Domestic Support Operations. Army Field Manual 100-19. Washington, D.C.: U.S, Department of the Army, July 1, 1993.

U.S. Department of Defense. DoD Antiterrorism Standards. Instruction Number 2000.16. Washington, D.C.: U.S. Department of Defense, 14 June 2001.

U.S. Department of Defense. DoD Antiterrorism/Force Protection (AT/FP) Program. Directive Number 2000.12. Washington, D.C.: U.S. Department of Defense, 13 April 1999.

U.S. Department of Defense. Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence. Handbook Number 0-2000.12-H. Washington, D.C.: U.S. Department of Defense, 19 February 1993.

U.S. Executive Office of the President. United States Intelligence Activities. Executive Order 12333. Washington, D.C.: Executive Office of the President, 4 December 1981.

U.S. Executive Office of the President. Establishing the Office of Homeland Security and the Homeland Security Council. Executive Order 13228. Washington, D.C.: Executive Office of the President, 8 October 2001.

U.S. General Accounting Office. Report to the Chairman, Special Oversight Panel on Terrorism, Committee on Armed Services, House of Representatives. "Combating Terrorism: Actions needed to Improve DOD Antiterrorism Program Implementation and Management." Washington, D.C.: U.S. General Accounting Office, 19 September 2001.

U.S Joint Chiefs of Staff. Combating Terrorism Readiness Initiatives Fund. Chairman of the Joint Chiefs of Staff Instruction 5261.01A. 1 August 1998. Available from <http://www.pseag.org/CWG_Documentation/CJCSI%205261-01A.html>. Internet. Accessed 9 December 2001.

U.S. Joint Chiefs of Staff. Joint Tactics, Techniques, and Procedures for Antiterrorism. Joint Publication 3-07.2. Washington, D.C.: U.S. Department of Defense, 17 March 1998.

U.S. Office of the Secretary of Defense. Policy Guidance for Intelligence Support to Force Protection. SECDEF Message DTG: 181700Z NOV 98. Washington, D.C.: U.S. Department of Defense, November 18, 1998.

U.S. Office of the Secretary of Defense. Report to Congress: Installation First Responder Preparedness. Washington, D.C.: U.S. Department of Defense, 26 March 2001.

Winograd, Erin Q. "U.S. Army Europe Chief: Force Protection Needs Demand Mental Agility." Inside the Army, 26 November 2001, 4-5.