

CJCS HANDBOOK 5260



Commander's Handbook for Antiterrorism Readiness



FOR OFFICIAL USE ONLY

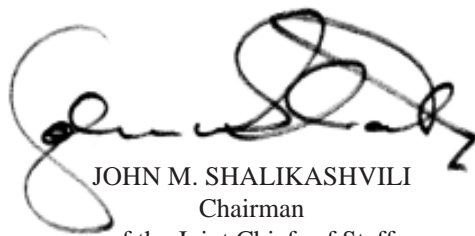
Foreword

Terrorism directed against America today is a by-product of our enhanced military status and capability, and will continue to be a challenge for all headers in the future. America's enemies have not gone away, they are simply less capable of waging conventional warfare against us. Guided by *Joint Vision 2010*, we must become preeminent in antiterrorism and force protection.



Several sweeping initiatives have been undertaken to institutionalize our commitment. I now serve as the principal adviser to the Secretary of Defense for all force protection matters. A flag officer-led, permanent Deputy Directorate for Combating Terrorism has been established to synchronize the renewed efforts of the entire Joint Staff. A force-wide, comprehensive assessment of physical security and force protection posture has been initiated, and funds for immediate improvements have been allocated. Additional mandatory training and professional education have been specified.

While all of these enhancements are important, the key remains you-the commander. This handbook was prepared to assist in meeting your responsibilities. It is the foundation for a new direction and mindset for combating terrorism. As we embrace this goal and execute our responsibilities, we will move toward fulfilling our sacred trust to protect those American sons and daughters under our care.



JOHN M. SHALIKASHVILI
Chairman
of the Joint Chiefs of Staff

Purpose

This handbook has been prepared to serve as a primary reference document for all officers with command authority within the Department of Defense. Used in conjunction with cited references, it will enable a commander to execute the following key components of antiterrorism readiness:

- Know intelligence and interagency antiterrorism (AT) architecture and information reporting procedures.
- Establish and/or comply with general physical security requirements and additional security measures at each THREATCON.
- Integrate AT awareness and concerns into operating procedures, plans, orders, and required exercises.
- Identify and ensure high-risk personnel, key staff and specialty personnel, and personnel deployed or deploying to areas with increased threat levels, receive appropriate AT training.
- Develop and sustain an AT awareness program for military personnel, civilian employees, and family members.
- Assess vulnerability and antiterrorism readiness.
- Ensure adequate funding is requested and applied in support of the AT measures listed above.

The American people will continue to expect us to win in any engagement, but they will also expect us to be more efficient in protecting lives and resources while accomplishing the mission successfully.

Joint Vision 2010

Contents

Chapter 1	<i>Nature of the Threat</i>
Chapter 2	<i>DOD Policy and Command Responsibilities</i>
Chapter 3	<i>Intelligence Access and Integration</i>
Chapter 4	<i>THREATCON</i>
Chapter 5	<i>Protecting the Force</i>
Chapter 6	<i>AT Training</i>
Appendix A	<i>DOD IG Antiterrorism Checklist</i>
Appendix B	<i>AT Essential Elements of Information</i>
Appendix C	<i>Memorandum of Understanding Between the Department of State and the Department of Defense on Overseas Security Support, 22 January 1992</i>
Appendix D	<i>Security Funding</i>
Appendix E	<i>Secretary of Defense Memorandum of 12 December 1995, Military Assistance to Civil Authorities</i>
Appendix F	<i>References</i>
 <i>Glossary</i>	



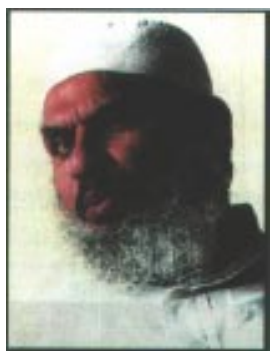
“...the Khobar Towers attack should be seen as a watershed event pointing the way to a radically new mindset and dramatic changes in the way we protect our forces deployed overseas from this growing threat.”

**Secretary Perry’s Report to the President
and Congress, 16 September 1996**

CHAPTER I

Nature of the Threat

Terrorist and criminal attacks on DOD personnel by individuals and organizations operating outside the formal command and control structure of national governments have claimed the lives of over 300 DOD-affiliated persons in the past 20 years. At least 600 DOD personnel have been injured in the same period.



Shaykh Umar Abd al-Rahman, convicted conspirator in the World Trade Center bombing.

The destruction of US Marine Headquarters at the Beirut Airport in October 1983 was the greatest loss of American military personnel attributed to a single terrorist act. Other attacks using terrorist methods, however, such as the World Trade Center bombing, the Tokyo subway nerve agent incident, and the truck bombing of the Oklahoma City Federal Building were equally horrific.

The incidents continue. On 13 November 1995, a truck bomb exploded in the parking lot of the Office of the Program Manager, Saudi Arabian National Guard (OPM/ SANG). Five Americans were killed and 35 US civilian and military personnel were injured. On 25 June 1996, a fuel truck

loaded with as much as 20,000 pounds of explosives was detonated outside the perimeter of the Khobar Towers complex in Dhahran. The blast, and resulting mass destruction, killed 19 US Service members and injured hundreds more. American military superiority, combined with increasing Third World interest in sophisticated, enhanced-effect weapons and weapons of mass destruction, demand that antiterrorism be a major focus well into the future.

No DOD-affiliated persons are immune from the risk of terrorist attack. Officers and enlisted personnel, civilian employees, and contractors have all been victims. Attacks have been conducted against DOD facilities, contractor facilities, and residences of DOD-affiliated persons. Even those personnel stationed in the continental United States are not immune to terrorist attack as underscored by the Oklahoma City incident. The Tokyo subway incident established precedence for the use of chemical materials.

The perpetrators of these attacks were terrorists. Their motivations were to intimidate and persuade the US Government to change its policies, or foreign governments to change theirs, or merely to gain notoriety for their cause. Yet, the use of terror to accomplish a goal is not new. Violent acts, or threats of violence, have been used throughout history to intimidate

individuals and governments into meeting terrorist demands. Terrorism is inexpensive, low-risk, highly effective, and allows the weak to challenge the strong.

Terrorism in the information age gains more notoriety now than major conflicts have had in the past. This is particularly true when targeted events, such as the Munich and Atlanta Olympics, already have worldwide media attention. The information age also has ushered in an era in which instructions for making explosives can be obtained instantly by anyone with a computer.

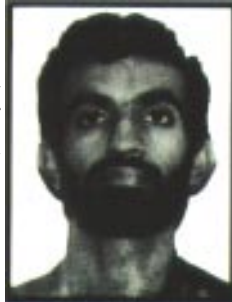
Individuals or groups use terrorism to gain objectives beyond their inherent capabilities. Employment of terrorist methods affords a weak nation an inexpensive form of warfare. Stronger nations use surrogates to employ terror while reducing their risk of retaliation and protecting their reputation. These nations feel insulated from retaliation as long as their relationship with the terrorist remains unproven.

Terrorism is employed throughout the spectrum of conflict to support political or military goals. Terrorists are an integral element in an insurgency and can supplement conventional warfighting. Terrorists can disrupt economic functions, demonstrate a government's incompetence, eliminate opposition leaders, and elevate social anxiety. The goal of terrorism is to project uncertainty and instability in economic, social, and political arenas.

Short-term terrorist goals focus on gaining recognition, reducing government credibility, obtaining funds or equipment, disrupting communications, demonstrating power, delaying the political process, reducing the government's economy, influencing elections, freeing prisoners, demoralizing and discrediting the security force, intimidating a particular group, and causing a government to overreact. Long-term goals are to topple governments, influence top level decisions, or gain legitimate recognition for a terrorist cause.

Terrorist Profile

The terrorist, urban guerrilla, saboteur, revolutionary, and insurgent are often the same depending upon the circumstance or political view. Although it is difficult to generalize a terrorist's character and motivation, a profile has been developed. Typically, terrorists are intelligent, well-educated, obsessed with initiating a change in the status quo, reared in middle class or affluent families, and 22 to 25 years of age. The ability to develop a terrorist profile provides a clearer image of the enemy and dispels dangerous misconceptions.



Ramzi Ahmed Yousef
terrorist and convicted World
Trade Center bomber

Terrorists are dedicated to their cause—even to the point of death. They are motivated by religion, prestige, power,

political change, or material gain, and believe they are an elite society that acts in the name of the people. Their dedication is evident in their education and training, arms and equipment, planning methods and ruthless execution. This dedication makes them a formidable enemy.

Terrorist Targets

Terrorists attack targets that are vulnerable, have a high psychological impact on a society, produce significant publicity, and demonstrate a government's inability to provide security. Both critical facilities and prominent individuals are potential terrorist targets. Military personnel and facilities have become increasingly appealing targets. Military facilities are a symbol of national power; a source of arms, ammunition, and explosives; and a prestigious target that adds to the terrorist's reputation. It is a dangerous mistake to think that high-ranking military personnel or those in key positions are the only terrorist targets.

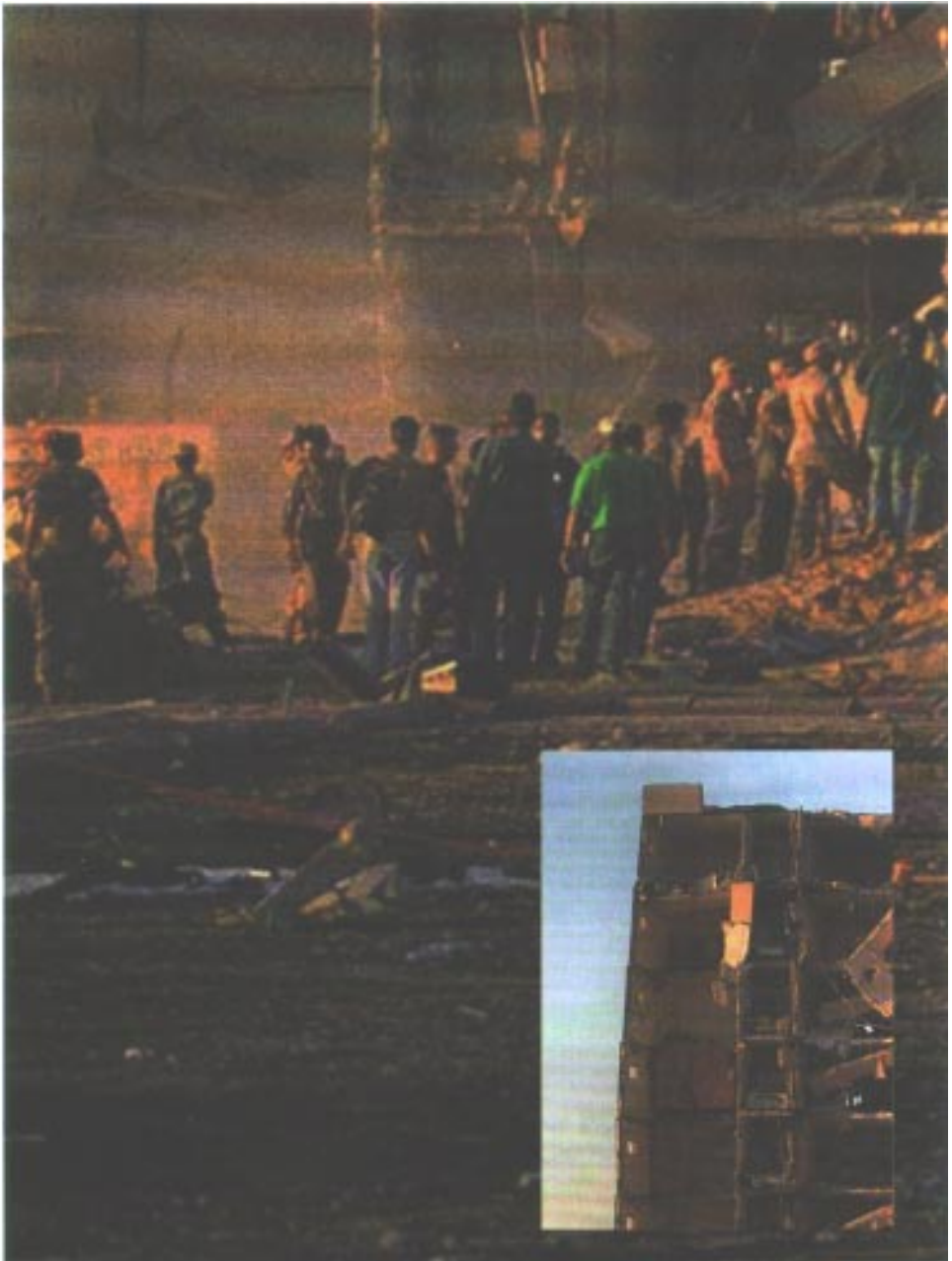
Terrorist Tactics, Training, and Equipment

Terrorist operations are meticulously planned. Prior to execution, detailed reconnaissance missions, training periods, and rehearsals ensure precise execution and minimize the risk of failure. Only select members of the terrorist command element have knowledge of the entire operation. Separate cells perform planning, reconnaissance,

support, and execution missions to prevent compromise. Contingency plans cover unforeseen events and alternate targets. Carefully staged movement of personnel and equipment helps avoid detection. Withdrawal, when considered, is planned in detail.

Intelligence confirms that terrorists are obtaining and employing sophisticated forgeries of travel and identity documents, and high-tech communications and surveillance equipment. Terrorists employ technology to defeat surveillance, inspection, and access control measures, and emplace explosives based on engineering analysis resulting in maximum yield. There is reason for concern that former Soviet-bloc weaponry, sensitive equipment stolen from Western countries, and stolen US military and civilian identification will all be employed in a terrorist attack against us.





“Those opposition includes extremist groups who are not only cold-blooded and fanatical, but also clever. They know that they cannot defeat us militarily, but they may believe they can defeat us politically, and they have chosen terror as the weapon to try to achieve this.”

**Secretary Perry’s Report to the President
and Congress, 16, September 1996**

CHAPTER 2

DOD Policy and Command Responsibilities

Introduction

US Government policy for combating terrorism is summarized in DOD 2000.12-H. The policy is clear and unambiguous—America will act in concert with other nations, and unilaterally when necessary, to resist terrorism by any legal means available. Our government will not make concessions to terrorists, including ransoms, prisoner releases or exchanges, or policy changes. Terrorism is considered a potential threat to national security, and other nations that practice or support terrorism “will not do so without consequence.”

Along with the Department of Defense, three other agencies coordinate US Government actions to resolve terrorist incidents:

The Department of State (DOS) is the lead Federal agency for responding to international terrorist incidents outside US territory, other than incidents on US flag vessels in international waters.

The Department of Justice (DOJ) is the lead Federal agency for responding to terrorist incidents within US territory. Unless otherwise specified by the Attorney General, the **Federal**



The terrorist bombing of a Pan Am jet over Lockerbie, Scotland on 21 December 1988 resulted in 274 deaths, including 11 persons on the ground.

Bureau of Investigation (FBI) will be the lead agency within DOJ for operational response to such incidents.

In instances of air piracy, the **Federal Aviation Administration (FAA)** has exclusive CONUS responsibility for coordination of any law enforcement activity affecting the safety of persons aboard aircraft. The FAA is responsible for communicating terrorist threat information to commercial air carriers and their passengers.

Department of Defense

DOD Directive 2000.12, revised and reissued 15 September 1996, establishes the Defense organization and responsibilities for combating terrorism.

Office of the Secretary of Defense (OSD). The Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) (SO/LIC) provides policy oversight, guidance and instruction, and coordinates physical security review and physical security equipment steering groups. ASD (SO/LIC) also hosts the annual *World-Wide AT Conference*. The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) oversees the efforts of the **Defense Intelligence Agency (DIA)** (see Chapter 3). Under Secretaries of Defense (Comptroller, Acquisition and Technology, Policy) play major supporting roles.

The Chairman of the Joint Chiefs of Staff (CJCS) is the principal adviser to the Secretary of Defense and serves as the focal point for all DOD force protection issues. The Chairman is responsible for the development of joint doctrine and professional military education, AT training and employment standards, reviewing Service doctrine and standards, and ensuring budget proposals support execution of AT policy. The Chairman assesses combatant command AT programs and ensures force protection is integrated into deployment and assignment considerations.

The Deputy Directorate for Combating Terrorism (J-34) was established to synchronize the efforts of the entire Joint Staff in combating terrorism. Led by a general/flag officer, this 37-member directorate has established the following goals:

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

The Secretaries of the Military Departments:

- Ensure the training of commanders on an integrated systems approach to physical security and force protection technology.
- Ensure that training on an integrated systems approach for force protection technology is included in planning for the acquisition of new facilities, AT systems, and equipment.
- Ensure that all Service installations and activities utilize DOD 2000.12-H to develop, maintain, and implement force protection efforts that familiarize personnel with DOD procedures, guidance, and instructions.
- Ensure that existing physical security, base defense, and law enforcement programs address terrorism as a potential threat to Service personnel and their families, facilities, and other DOD material resources.
- Ensure each installation or base and/or ship has the capability to respond to a terrorist incident.

- Ensure installations or bases and/or ships conduct operational or command post exercises annually.

- Ensure every commander, regardless of echelon or branch of Service, plans, resources, trains, exercises, and executes antiterrorism measures outlined in referenced DOD and Joint Pubs.

- Ensure the training of individuals and specified personnel (see Chapter 6).

Combatant Commanders with territorial responsibilities:

- Review the AT force protection status of all military activities, including DOD contracting activities, within the AOR, IAW DOD 2000.12-H. Service component and subordinate commands can conduct the review, but the CINC remains responsible and will be rendered a formal report.

- Assess command relationships with component commands and JTFs to ensure adequate protection from terrorist attack.

No information contained in this handbook or cited references shall detract from, nor be construed to conflict with, the inherent responsibility of commanders to protect military installations, equipment, or personnel under their command.

- On a periodic basis, assess the AT force protection of all non-combatant military activities (Attaches, Security Assistance Organizations, etc.) within the AOR, whose security is provided by DOS, and recommend whether force protection should be assigned to the CINC.

- Using DOD 2000.12-H, establish command policies and programs for the protection of DOD personnel and their families, facilities, and other DOD material resources from terrorist attacks.

- Ensure that AT countermeasures are being coordinated with host-country agencies at all levels.

- Assist any DOD element, within the AOR, in implementing required programs.

- Serve as the DOD point of contact with US Embassies and host nation officials on matters involving AT policies and measures.

- Ensure the training of individuals and specified personnel (Chapter 6).

- Designate an office staffed with trained personnel to supervise, inspect, test, and report on the base AT programs within the AOR.

- Integrate AT incidents into training scenarios for field and staff exercises. These exercises should be linked to specific tasks in the Universal Joint Task List, CJCSM 3500.004a.

Commanders in Chief with global missions, such as **USCINCSOC**, **USCINCTRANS**, **USCINCSpace**, and **USCINCSTRAT**, execute command responsibilities while assisting regional CINCs with their territorial responsibilities.

Domestic Policy

It is DOD policy to support Federal, state, and local law enforcement agencies to the extent allowed by public law. Support may be provided on and off military installations within these limits.

Although DOJ is the lead agency designated for coordinating US Government actions to resolve terrorist incidents within the United States, installation commanders have inherent authority to take reasonably necessary and lawful measures to maintain law and order on installations and to protect military personnel, facilities, and property. This authority also includes the removal from or the denial of access to an installation or site of individuals who threaten the orderly administration of the installation or site. Commanders should immediately seek the advice of legal personnel when this type of situation evolves.

The **FBI** is the lead operational agency for response to terrorist incidents occurring in the United States. DOD support can be provided under two authorities:

- Routine support can be provided under the provisions of DODD 5525.5,

SL leader Abimael Guzman
incarcerated Sept. 1992.



US Embassy Lima after SL
detonated a car bomb
July 27, 1993.

• Domestic terrorism support is furnished under the provisions of DODD 3025.1, “Military Support to Civil Authorities”; and DODD 3025.12, “Military Assistance for Civil Disturbances.” Within the territory of the United States, use of military forces to conduct law enforcement actions is restricted by law, unless authorized by an Executive order directing the Secretary of Defense to take action within a specified civil jurisdiction, under specific circumstances.

International Policy

“DOD Cooperation with Civilian Law Enforcement Officials.” Historically, the Department of Defense has provided a wide variety of routine and specialized support to civilian law enforcement agencies.

DOD activities outside of US territory are bound by international treaties and agreements. While Status of Forces Agreements (SOFA) are the most common example, other bilateral and multilateral stationing agreements impact on US forces’ actions to prevent.



Results of a terrorist bombing on a crowded Algiers street, targeting independent and unsympathetic newspaper publishers, killing 17 people and injuring 87 others.

and react to terrorist incidents. Such agreements define the authorities and responsibilities of the host country and of US forces based within the host country. These include agreements concerning security, safety, use of facilities, sharing of criminal intelligence information, rules for use of force, and other matters of mutual concern.

Primary responsibility for responding to overseas terrorist threats or attacks rests with the host country. Commanders should carefully review and ensure they clearly understand DOD Instruction 5210.84, “Security of DOD Personnel at US Missions Abroad.” The host country has a legitimate interest in and right to enforce the law and maintain security, even on US installations, within its borders. International agreements allow the US to exercise authority on US installations. Even if the host country refuses to protect US installations, the right of self-defense to protect US facilities, property, and personnel is not infringed.

The US commander retains the responsibility for the safety and security of personnel and property on US installations outside US territory. Generally, stationing arrangements grant the United States the right to take necessary lawful measures to ensure the security of US installations and personnel. The following considerations impact this decision process:

- Applicable directives and regulations for security of US military

installations, personnel, and facilities inside the United States also apply outside US territory, except where made inapplicable in whole or in part by international agreements.

- The United States may be obligated by international agreement to cooperate with host-country authorities and allow them access to US installations to protect existing host-country interests subject to US security considerations.

- Generally, military regulations concerning rules for the use of force and rules for carrying firearms must comply with both US and host nation standards.

- The United States retains primary criminal jurisdiction over US personnel committing criminal acts while performing official duties, and personnel are generally protected from civil liability while performing official duties. Failing to follow US or host-nation rules, such as those for the carrying of firearms, however, may fall outside the scope of “official duties” and subject US personnel to foreign criminal and civil jurisdiction.

CHAPTER 3

Intelligence Access and Integration

Introduction

The continual threat of terrorist activity targeted against US Government personnel, facilities, assets, and interests has resulted in the development of a significant organizational structure to collect, analyze, and disseminate intelligence.

Collection

The **FBI** is the lead agency for acquiring terrorist information and intelligence within the United States. The **CIA** is the lead agency for acquiring such information in foreign countries. Constitutional considerations restrict the ability of DOD personnel to collect information on unaffiliated persons with the United States. DOD intelligence and counterintelligence components may collect and retain information that identifies a US person only if it is necessary to the conduct of a function assigned to the collecting component, and only if that information falls within specific categories. Commanders and their legal advisers ensure that intelligence personnel, and others, follow the substantive procedural requirements of the following references while conducting intelligence activities:

- Public Law 95-511, “Foreign Intelligence Surveillance Act of 1978.”
- Executive Order 12333, “United States Intelligence Activities,” 4 December 1981.
- DOD Directive 5240.1, “DOD Intelligence Activities,” 25 April 1988.
- DOD Directive 5240.1-R, “Activities of DOD Intelligence Components That Affect United States Persons,” December 1982.
- Service Regulations.

Substantial technical collection means (SIGINT, ELINT), often designed to be employed against a conventional opposing force, exist and continue to be developed. Even when these means are available and effective, human intelligence (HUMINT) remains a key component of all-source intelligence collection. Each Service maintains field-level intelligence and counterintelligence agents who develop their own sources. Primary sources, however, are often our own Service personnel. Commanders must encourage intelligence prebriefing, reporting, and debriefing of guards, law enforcement and investigative personnel, and others in a position to monitor potential terrorists and terrorist activity.

Intelligence liaison at all levels, with US and host-nation intelligence and law enforcement agencies, provide commanders an expanded picture of the AOR, and extend the arms of the entire US antiterrorism effort.

Analysis: Organization

The Community Counterterrorism Board (CCB) is responsible for coordinating national intelligence agencies concerned with combating international terrorism. These organizations include the CIA, DOS, DOJ, FBI, Department of Energy (DOE), and Department of Transportation (US Coast Guard). DIA represents the Department of Defense on this board, although the Services regularly participate.

The Secretary of Defense has directed DIA to establish and maintain an all-source terrorism intelligence fusion center. The **AT Watch Cell** and an on-call **Crisis Response Cell** have been established at the National Military Command Center (NMCC) and are jointly staffed by personnel from J-34 and the J2/DIA Threat Warning Division. The mission of the Watch Cell is to provide senior military leadership including CINCs with a focused assessment of terrorist indications and warnings (I&W) worldwide. **The AT Watch Cell's primary goal is to translate I&W and intelligence into indicators which trigger operational actions and enhance force protection measures.**

We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to the same.

Joint Vision 2010

The Secretaries of the Military Departments are directed to ensure that a capability exists to receive, evaluate from a Service perspective, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack. Service agencies include the Army Counter-intelligence Center (ACIC), Navy Antiterrorism Alert Center (NAVATAC), US Air Force Office of Special Investigations (AFOSI), and Headquarters US Marine Corps, Counterintelligence/HUMINT Branch (HQMC (CIC)). Each Service operates a 24-hour operations center and maintains open lines of communications with the NMCC AT Watch Cell and combatant commands.

Analysis: Threat Levels

DOD has developed a methodology to assess the terrorist threat to DOD personnel, facilities, material, and interests. Six factors are used in shaping the collection and analysis of information.

Existence. A terrorist group is present, assessed to be present, or able to gain access to a given country or locale.

Capability. The acquired, assessed, or demonstrated level of capability for a terrorist group to conduct attacks.

Intentions. Recent demonstrated anti-US terrorist activity, or stated or assessed intent to conduct such activity.

History. Demonstrated terrorist activity over time.

Targeting. Current credible information on activity indicative of preparations for specific terrorist operations.

Security environment. The internal political and security considerations that impact on the capability of terrorist elements to carry out their intentions.

Threat levels are obtained based on the presence of a combination of the factors listed above. **Terrorist threat levels do not address when a terrorist attack will occur and do not specify a THREATCON status**

(Chapter 4). Issuance of a terrorist threat-level judgment is not a warning notice. Formal terrorism warning notices are issued separately.

CRITICAL. Factors of Existence, Capability, and Targeting must be present. History and Intentions may or may not be present. CRITICAL is differentiated from all other terrorist threat levels because it is the only one in which credible information identifying specific DOD personnel, facilities, assets, or interests as potential targets of attack is present. Although particular action is not specified, a CRITICAL threat level compels local commanders to take appropriate protective measures.

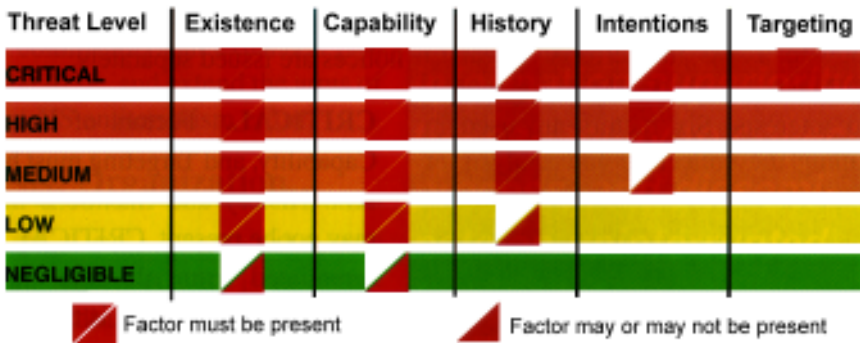
HIGH. Factors of Existence, Capability, History, and Intentions must be present, but analysts lack specific targeting information.

MEDIUM. Factors of Existence, Capability, and History must be present. Intentions may or may not be present. Threat level MEDIUM and threat level HIGH are similar in that data for the factors Evidence, History, and Capability exist.

LOW. Existence and Capability must be present. History may or may not be present.

NEGLIGIBLE. Existence and/or Capability may or may not be present.

Threat Analysis Factors



DOD-Level Determination of Terrorist Threat Level

NOTE: These terrorist threat levels must not be confused with joint rear area threat levels (as defined in Joint Pub 3-10) or terrorist threat conditions (THREATCONs).

Dissemination

DIA provides a wide range of terrorism intelligence products to DOD components, including daily awareness products, longer-range assessments, and estimates of terrorist activities. Service agencies also provide periodic terrorism products and threat data to supported commanders. The CINCs, through their J-2s and in consultation with the DIA, embassy staffs, and applicable host-nation authorities, obtain, analyze, and report information specific to their AOR.

The primary intelligence mission in support of the DOD combating terrorism program, however, is terrorism warning. Terrorist threat warning is accomplished for the Department of Defense using two mechanisms.

- The national intelligence community issues fully coordinated **Terrorist Threat Alerts** and **Terrorist Threat Advisories**. The Executive Coordinator of the Community Counterterrorism Board, is responsible for coordinating terrorism threat warnings outside CONUS. The **FBI** is responsible for coordinating and issuing warnings for domestic threats.

- **The Defense Indications and Warning System (DIWS)** comprises a second, independent system in which DIA, combatant commands, and Services may initiate unilateral threat warnings. These are termed **Defense Terrorism Warning Reports (TWRs)**.

Service components and Defense agencies also have the right to notify their members of terrorist threats

independently. If a DOD component intelligence activity receives information that leads to an assessment of an imminent terrorist attack, it may exercise its right to issue a unilateral warning to units, installations, or personnel identified as targets for the attack. If the DOD component intelligence activity issues a unilateral warning, it must label threat information disseminated as a unilateral judgment and will inform DIA of its action.

Terrorism warnings are issued when specificity of targeting and timing exist, or when analysts have determined that sufficient information indicates US personnel, facilities, or interests are being targeted for attack. Warnings need not be country specific and can cover an entire region. Success of the system depends upon collection, and the ability of analysts to recognize the indicators for an

attack. DIWS Terrorism Warning Reports are unambiguous—it is clear to the recipients they are being warned. Warnings are intended for distribution up, down, and laterally through the chain of command. Warnings of impending terrorist activity are likely to have national implications, and when issued, are reported to the National Command Authorities.

Under our *no double standard policy*, no terrorist threat warning will be issued solely to US Government personnel if the general public is included in, or can be construed to be part of, terrorist targeting. Terrorist threat warnings may be issued exclusively within government channels only when the threat is to government targets. DOS is the sole approving authority for releasing terrorist threat information to the public.



CHAPTER 4 THREATCON

Whereas the Terrorist Threat Level is an intelligence community judgment about the likelihood of terrorist attacks on DOD personnel and facilities, the **THREATCON** is the principal means a commander has to apply an operational decision on how to guard against the threat. Ultimately it is the commander who must weigh the information and balance increased security measures with the loss of effectiveness during prolonged operations and the accompanying impact on quality-of-life.



THREATCONs are selected by assessing the terrorist threat, the capability to penetrate existing physical security systems at an installation, the risk of terrorist attack to which DOD facilities and personnel expose themselves, the ability of the installation or units to carry on with missions even if attacked, and the criticality to DOD missions of assets to be protected.

THREATCONs can be established by commanders at any level, and subordinate commanders can establish a higher THREATCON if local conditions warrant doing so. THREATCON measures are mandatory when declared and can be supplemented by additional measures. The declaration, reduction, and cancellation of THREATCONs remain the exclusive responsibility of the commanders issuing the order.

THREATCON NORMAL exists when there is no known threat.

THREATCON ALPHA exists when there is a general threat of possible terrorist activity against installations and personnel. The exact nature and extent are unpredictable and circumstances do not justify full implementation of

FOR OFFICIAL USE ONLY

THREATCON BRAVO. However, it may be necessary to implement selected THREATCON BRAVO measures as a result of intelligence or as a deterrent. THREATCON ALPHA must be capable of being maintained indefinitely.

THREATCON BRAVO exists when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing hardship, affecting operational capability, or aggravating relations with local authorities.

THREATCON CHARLIE exists when an incident occurs or when intelligence is received indicating that some form of terrorist action is imminent. Implementation of this measure for longer than a short period of time will probably create hardship and affect peacetime activities of a unit and its personnel.

THREATCON DELTA exists when a terrorist attack has occurred, or when intelligence indicates that a terrorist action against a specific location is likely. Normally, this THREATCON is declared as a localized warning.

Once a THREATCON is declared, the following security measures are mandatory and implemented

immediately. Commanders are authorized and encouraged to supplement these measures.

THREATCON ALPHA

Measure 1: At regular intervals, remind all personnel and dependents to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for unidentified vehicles on or in the vicinity of US installations. Watch for abandoned parcels or suitcases and any unusual activity.

Measure 2: Have the duty officer or personnel with access to building plans and plans for area evacuations available at all times. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on call and readily available.

Measure 3: Secure buildings, rooms, and storage areas not in regular use.

Measure 4: Increase security spot checks of vehicles and persons entering the installation and unclassified areas under the jurisdiction of the United States.

Measure 5: Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

Measure 6: As a deterrent, apply measures 14, 15, 17, or 18 from THREATCON BRAVO individually or in combination.

FOR OFFICIAL USE ONLY

Measure 7: Review all plans, orders, personnel details, and logistic requirements related to the introduction of higher THREATCONs.

Measure 8: Review and implement security measures for high-risk personnel, as appropriate.

Measure 9: Spare.

THREATCON BRAVO

Measure 10: Repeat measure 1 and warn personnel of any other potential form of terrorist attack.

Measure 11: Keep all personnel involved in implementing antiterrorist contingency plans on call.

Measure 12: Check plans for implementation of the next THREATCON.

Measure 13: Move cars and objects (e.g., crates, trash containers) at least 25 meters from buildings, particularly buildings of a sensitive or prestigious nature. Consider centralized parking.

Measure 14: Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

Measure 15: At the beginning and end of each workday and at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

Measure 16: Examine mail (above the regular examination process) for letter or parcel bombs.

Measure 17: Check all deliveries to messes, clubs, etc. Advise dependents to check home deliveries.

Measure 18: Increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense and to build confidence among staff and dependents.

Measure 19: Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.

Measure 20: At an early stage, inform members of local security committees of actions being taken. Explain reasons for actions.

Measure 21: Physically inspect visitors and randomly inspect their suitcases, parcels, and other containers.

Measure 22: Operate random patrols to check vehicles, people, and buildings.

Measure 23: Protect off-base military personnel and military transport in accordance with prepared plans. Remind drivers to lock vehicles and check vehicles before entering or driving.

Measure 24: Implement additional security measures for high-risk personnel as appropriate.

Measure 25: Brief personnel who may augment guard forces on the use of deadly force.

Measures 26-29: Spares.

FOR OFFICIAL USE ONLY

THREATCON CHARLIE

Measure 30: Continue or introduce all measures listed in THREATCON BRAVO.

Measure 31: Keep all personnel responsible for implementing antiterrorist plans at their places of duty.

Measure 32: Limit access points to absolute minimum.

Measure 33: Strictly enforce control of entry. Randomly search vehicles.

Measure 34: Enforce centralized parking of vehicles away from sensitive buildings.

Measure 35: Issue weapons to guards. Local orders should include specific orders on issue of ammunition.

Measure 36: Increase patrolling of the installation.

Measure 37: Protect all designated vulnerable points. Give special attention to vulnerable points outside the military establishment.

Measure 38: Erect barriers and obstacles to control traffic flow.

Measure 39: Spares.

THREATCON DELTA

Measure 40: Continue or introduce all measures listed for THREATCONs BRAVO and CHARLIE.

Measure 41: Augment guards as necessary.

Measure 42: Identify all vehicles within operational or mission support areas.

Measure 43: Search all vehicles and

their contents before allowing entrance to the installation.

Measure 44: Control access and implement positive identification of all personnel.

Measure 45: Search all suitcases briefcases, packages, etc., brought into the installation.

Measure 46: Control access to all areas under the jurisdiction of the United States.

Measure 47: Frequent checks of building exteriors and parking areas.

Measure 48: Minimize all administrative journeys and visits.

Measure 49: Coordinate the possible closing of public and military roads and facilities with local authorities.

Measure 50: Spare.

Random Antiterrorism Measures (RAM)

Random Antiterrorism Measures complement and supplement, but do not replace, the DOD THREATCON System. RAM is an effective OPSEC measure that enhances security and greatly limits the ability of terrorists to determine patterns of security and responses. These measures, such as random vehicle searches and ID card checks, commonly are taken from higher THREATCON measures to supplement lower ones. RAM can assist in vulnerability analysis, train security forces, raise general AT consciousness, and are easier to sustain.

FOR OFFICIAL USE ONLY

CHAPTER 5

Protecting the Force



Force Protection, by definition, has a much broader scope than antiterrorism. Force protection is defined as *the security program designed to protect soldiers, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism (antiterrorism and counterterrorism), physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs.* All the components of force protection, however, can have a major impact on a command's antiterrorism readiness.

DOD 2000.12-H [Handbook], "Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence," details command planning and response to terrorism; physical security requirements for installations, facilities, work and residential structures; and personnel security measures for individuals and designated personnel. **The 15 September 1996 revision to DOD Directive 2000.12 applies the information contained in 12-H as the DOD standard.** The handbook is currently undergoing broad staffing for revision.

Physical Security programs involve *physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.* Physical security measures deter, detect, and defend against threats from terrorists, criminals, and unconventional forces. Measures include fencing and perimeter stand-off space, lighting and sensors, vehicle barriers, blast protection, intrusion detection systems (IDS) and electronic surveillance, and access control devices and systems. These methods are augmented by procedural measures such as security checks, inventories, and inspections. Physical security measures, like any defense, should be overlapping and deployed in depth.

Required physical security measures are detailed in referenced DOD publications and Service regulations. As our technological capability

increases, so does the need to apply these advances to combat terrorism. This effort was emphasized during a recent Force Protection Technology Symposium with military and industry, sponsored by the Joint Staff and Defense Special Weapons Agency. The Chairman of the Joint Chiefs of Staff delivered the keynote address.

Operations Security is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations *and other activities* to:

- Identify those actions that can be observed by adversary intelligence systems.
- Determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
- Select and execute measures that eliminate or reduce to an accept-

To protect our vital national interests we will require strong armed forces, which are organized, trained, and equipped to fight and win against any adversary at any level of conflict.

Joint Vision 2010

able level the vulnerabilities of friendly actions to adversary exploitation.

OPSEC has always been an integral part of military doctrine, but the challenge for commanders is to apply these time-tested principles to combat terrorism. Effective OPSEC measures minimize the “signature” of DOD activities, avoid set patterns, and employ deception when patterns cannot be altered. Although strategic OPSEC measures are important, **the most effective methods manifest themselves at the lowest level.** Terrorist activity is discouraged by varying patrol routes, staffing guard posts and towers at irregular intervals, and conducting vehicle and pedestrian searches and identification checks on a set but unpredictable pattern. While such activity during peak traffic periods can be inconvenient and frustrating to authorized personnel, commanders must be cognizant that it is during these periods that DOD activities are most vulnerable.

Commanders cannot underestimate the modern terrorist’s technical collection capability. Terrorists, particularly when state-sponsored, are capable of employing electronic eavesdropping devices, communications intercept equipment, and advanced, remote imagery collection.

Force protection measures are a challenge for commanders and public affairs officers when dealing with the

media, the general public, and host-nation authorities. The Public Affairs Officer, like all staff members, is a key player in the program and works to have the media’s interest serve the command. The media can assist with AT awareness while accurately portraying command measures as vital force protection efforts.

A major by-product of measures designed to defeat terrorists is effectiveness against other criminal threats. The exposure of the DOD population to drug trafficking and gang violence can be limited while simultaneously protecting against a calculated terrorist attack.

Personnel Security measures range from the common-core, general measures of antiterrorism, to specialized personal protective services. They include common-sense (but hard to enforce) rules of on- and off-duty conduct, to protective clothing and equipment, hardened vehicles and facilities, dedicated guard forces, and duress alarms. Events bear out that DOD personnel of all ranks are vulnerable to terrorist targeting and attack, particularly while traveling and off-duty. While in that status in a foreign country, particularly on a temporary visit or port call, it is vital to consider:

- Coordination with host-nation law enforcement and US Embassy/Consulate staff to determine the

BE ALERT KEEP A LOW PROFILE BE UNPREDICTABLE

latest threat status, and potential trouble spots.

- Joint US/host-nation law enforcement and courtesy patrols.
- Enforcement of the *two-person* rule. Requiring personnel to use the buddy system is an effective deterrent to terrorism and general street crime.

Conclusion

Force protection is an integrated effort on the part of staffs of all units. Commanders of units and installations must have the mindset that combating terrorism is not just the responsibility of military law enforcement personnel. These personnel are another component of a successful team effort.



CHAPTER 6

AT Training

To institutionalize policy and procedure, antiterrorism will be an integral part of training and education in joint and Service schools, specialty courses, and units. Training is required for all DOD military and civilian personnel.

DOD Instruction 2000.14, “DOD Combating Terrorism Program Procedures,” requires AT threat awareness and personal protection training in all officer and enlisted initial entry training. Basic branch qualification courses will then train this task to more specific, branch- or occupation-related functions. NCO leadership, officer staff and command, and joint schools will conduct training and exercises designed to integrate staff functions for combating terrorism.



Specialty Courses. Commands are required, no less than annually, to **review high-risk positions and identify high-risk personnel.** These personnel must attend the *Individual Terrorism Awareness Course* (5 days) at the JFK Special Warfare Center and School at Fort Bragg, North Carolina, or a Service-approved equivalent course.

Personnel designated as **installation or base Antiterrorism Officers** will attend the *Combating*

Terrorism on Military Installations and/or Bases Course (5 days) at the US Army Military Police School, Fort McClellan, Alabama, or an equivalent course. Combatant commands are required to designate a staff office responsible for antiterrorism and ensure that at least one individual has received this formal, resident training. Unit/ship Antiterrorism Officers are currently required to be designated only if deploying to a high-threat area. Because the area of operations and local threat conditions can change at any time, it is strongly encouraged

to designate and train these officers in advance.

Personnel deploying to high threat or potentially high threat areas, should attend the *Dynamics of International Terrorism Course* at the US Air Force Special Operations School at Hurlburt Field, Florida, or some other formal course taught by Service-qualified instructors.

DOD Instruction 2000.14 includes other specialty course listings, including the *Antiterrorism Instructor Qualification Course* and other specialty courses at JFK and Hurlburt Field, evasive driving courses for general/flag officers and their drivers, and legal and intelligence specialty courses offered at the US Army Judge Advocate and Intelligence Schools, respectively.

Law enforcement specialty courses include *Special Reaction Team*, *Physical Security/Crime Prevention*, *Hostage Negotiation*, and *Protective Services* courses at the US Army Military Police School at Fort McClellan.

The US Army Corps of Engineers offers a *Security Engineering* course for both security and engineering personnel, taught at various locations by the staff of the Protective Design Center, Omaha District. Huntsville District offers a similar course for electronic detection design.

Additional joint courses may be found in the Joint Course Catalog pub-

lished by the Joint Warfighting Center, Fort Monroe, Virginia.

Unit-Level Training. Services are tasked with providing periodic training on terrorist threat and personnel protection principles and techniques; instituting awareness programs designed to raise the awareness of Service personnel and their family members to the general terrorist threat; and teaching measures that reduce personal vulnerability. CINCs are charged with developing and maintaining an antiterrorism program, identifying AOR-specific antiterrorism training requirements for personnel prior to arrival, and conducting field or staff training at least annually to exercise AT plans.

The Secretary of Defense approved a Downing Task Force recommendation that all personnel, military or civilian, deploying overseas whether on temporary or permanent duty, be given general and AOR-specific AT training. The Commander In Chief, US Atlantic Command, at the request of the Chairman of the Joint Chiefs of Staff, led a combined combatant command/Service effort to determine predeployment training requirements. The resulting, CJCS-approved training concept identifies baseline training requirements for all individuals, and additional training for unit AT personnel and senior leadership. This policy will be included in pending updates to DOD Directives.

APPENDIX A

DOD IG Antiterrorism Checklist

This document was prepared by the Inspector General, Department of Defense, as a vehicle by which to survey DOD components regarding their antiterrorism readiness at a given point in time. The checklist was not intended as a means of measuring adequacy of antiterrorism efforts expended by those DOD components, was not intended to be a dynamic or “living” document, and should not be used alone. The checklist should only be used in conjunction with other assessment techniques available to those components.

DOD SPECIAL INTEREST ITEM: ANTITERRORISM READINESS

COMBATING TERRORISM (ANTITERRORISM/ COUNTERTERRORISM)

	<u>Yes</u>	<u>No</u>	<u>N/A</u>
1. Does the organization have a combating terrorism program in accordance with (JAW) DODD 1 2000.12 and/or the Service implementing document?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Does the organization have a combating terrorism plan IAW DODD 2000.12 and/or the Service implementing document?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Is antiterrorism (AT) planning integrated into overall force protection planning as recommended by DOD 2000.12-H?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Has the combating terrorism plan been coordinated with foreign, state, and local law enforcement agencies as recommended by DOD 2000.12-H?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ANTITERRORISM PLANNING AND OPERATIONS

5. Does the organization have the most current version of all appropriate directives, instructions, regulations, and other pertinent documents?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
---	--------------------------	--------------------------	--------------------------

1 DOD Directive

	<u>Yes</u>	<u>No</u>	<u>N/A</u>
6. Has the organization designated an antiterrorism officer and provided for their training IAW DODINST 2 2000.14 and/or the Service implementing document?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. Has the organization established an AT awareness program IAW DODD 2000.12?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8. Do all members of the organization receive periodic terrorism awareness briefings IAW DODD 2000.12?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9. Has the organization conducted an AT exercise within the last 12 months IAW DODINST 2000.14 and/or the Service implementing document?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10. Have terrorism scenarios been integrated into training exercises IAW DODINST 2000.14 and/or the Service implementing document?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11. Has the organization performed either a vulnerability assessment or a risk analysis as recommended by DOD 2000.12-H?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12. a) Has a prioritized list of Mission Essential Vulnerable Areas been established as recommended by DOD 2000.12-H and Service guidance?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b) Is there a plan of action and have milestones been established for addressing vulnerable areas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13. a) Does the organization have a crisis management team as recommended by DOD 2000.12-H?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b) Does it have proper staff representation and has it met within the last 90 days?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c) Has the organization followed guidance of DOD 2000.12-H, Chapter 15, "Terrorism Crisis Management Planning and Execution?"	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ANTITERRORISM FOR UNIT DEPLOYMENTS

14. a) Are there well-defined and located-specific pre-deployment AT requirements as recommended by DOD 2000.12-H and Joint Pub 3-07.2?
- b) Do they provide for pre-deployment threat awareness training?
- c) Do they identify key elements for additional protection after deployment?
- d) Do they ensure against interruption of the flow of threat information to deployed units?

THREAT INFORMATION: COLLECTION AND DISSEMINATION

15. Do procedures exist to allow for the timely dissemination of terrorist threat both during and after duty hours IAW DODD 2000. 12?
16. Does the organization have a travel security program and does it provide threat information briefings on a regular basis IAW DODD 2000.12?
17. a) Has collection and dissemination of terrorist information been reviewed by the Commander in the last year?
- b) Did he assess it as adequate?
18. Is the threat assessment current IAW DODD 2000. 1 2?
19. Does the organization receive recurring threat updates IAW DODD 2000. 1 2 and/or the Service implementing document?

- | | <u>Yes</u> | <u>No</u> | <u>N/A</u> |
|--|--------------------------|--------------------------|--------------------------|
| 20. Is the intelligence analysis at the installation or deployed location a blend of all appropriate intelligence disciplines and does the intelligence officer/NCO understand the sources of the information? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 21. Are there indications all available information is not being collected? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

PHYSICAL SECURITY

- | | | | |
|--|--------------------------|--------------------------|--------------------------|
| 22. Does the organization have a physical security plan IAW DODD 2000.12 and DODD 5200.8? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 23. Are AT protective measures incorporated into the physical security plan as recommended by DOD 2000.12-H? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 24. Have procedures been established to ensure that all military construction projects are reviewed at the conceptual stage to incorporate physical security, antiterrorist, or protective design features IAW with DODD 5200.8-R? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

LAW ENFORCEMENT AGENCY INVOLVEMENT

- | | | | |
|--|--------------------------|--------------------------|--------------------------|
| 25. Is Law Enforcement Agency developed information shared and blended with Intelligence information as recommended by DOD 2000.12-H? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 26. Is there a mutual understanding between all local agencies that might be involved in a terrorist incident on the installation regarding authority, jurisdiction, and possible interaction as recommended by DOD 2000.12-H? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

FUNDING

	<u>Yes</u>	<u>No</u>	<u>N/A</u>
27. Were AT funding requirements identified during the POM cycle? Please provide the detailed information involved in the POM submission.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
28. Have required AT enhancements been identified and prioritized?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
29. Are there shortfalls in AT funding projected in FY XXXX? If so, what are they? _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
30. a) What percentage of requested funding was received in FY XXXX [previous FY] ? _____%	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b) Amount requested? \$ _____			
c) Amount received? \$ _____			
31. Has the lack of funding adversely impacted the organization's AT program? If yes, please comment. _____ _____ _____ _____ _____ _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

REFERENCES:

DODD 2000.12: "DOD Combating Terrorism Program," September 15, 1996

DOD 2000.12-H: "Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence," February, 1993

DODINST 2000.14: "DOD Combating Terrorism Program Procedures," June 15, 1994

DODD 5200.8: "Security of Military Installations and Resources," April 25, 1991

DODD 5200.8-R: "Physical Security Program," May 1991

Joint Pub 3-07.2: "Joint Tactics, Techniques, and Procedures (JTTP) for Antiterrorism," June 25, 1993

APPENDIX B

AT Essential Elements of Information

Essential Elements of Information

The following terrorist considerations should be used in developing essential elements of information:

- Organization, size, and composition of group
- Motivation
- Long- and short-range goals
- Religious, political, and ethnic affiliations
- International and national support (e.g., moral, physical, financial)
- Recruiting methods, locations, and targets (e.g., students)
- Identity of group leaders, opportunities, and idealists
- Group intelligence capabilities
- Sources of supply and support
- Important dates (e.g., religious holidays)
- Planning ability
- Degree of discipline
- Preferred tactics and operations
- Willingness to kill
- Willingness to self-sacrifice
- Group skills (e.g., sniping, demolition, masquerade, industrial sabotage, airplane or boat operations, tunneling, underwater maneuvers,

electronic surveillance, poisons, and contaminants)

- Equipment and weapons (on hand and required)
- Transportation (on hand and required)
- Medical support availability

Guidance in Development of Terrorist Threat Estimate

- Determine installation and unit mission. Include any implied missions related to security.
- Develop installation and unit assessment.
- Develop installation vulnerability assessment.
- Develop criticality assessment.
- Determine feasibility of spreading or combining key assets and infrastructures. Input this data into the Installation Base Master Plan.
- Determine if redundancy of key assets and infrastructures exists on the installation or within the geographic area.
- Develop procedural plans in the event current assets are disabled.
- Develop damage control procedures to minimize the effects of damage or destruction to key assets and infrastructures.

-
-
- Develop a threat assessment in order to determine:
 - (1) Existence, or potential existence, of a terrorist group.
 - (2) Acquired, assessed, or demonstrated terrorist capability level.
 - (3) Stated or assessed intentions toward US forces.
 - (4) Previously demonstrated terrorist activity.
 - (5) Probable terrorist target based on current information.
 - (6) Internal political and security considerations.

APPENDIX C
Memorandum Of Understanding Between
The Department Of State
And The
Department Of Defense
On
Overseas Security Support
22 January 1992

The Departments of State and Defense agree to the following provisions regarding overseas security services and procedures, in accordance with the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (P.L. 99-399).

I. AUTHORITY AND PURPOSE

The Omnibus Diplomatic Security and Antiterrorism Act of 1986, hereafter referred to as the Omnibus Act, requires the Secretary of State, in consultation with the heads of other federal agencies having personnel or missions abroad, where appropriate and within the scope of resources made available, to develop and implement policies and programs, including funding levels and standards, to provide for the security of United States Government operations of a diplomatic nature. Such policies and programs shall include:

- A. Protection of all United States Government personnel on official duty abroad (other than those personnel under the command of a United States area military commander) and their accompanying dependents, and

- B. Establishment and operation of security functions at all United States Government missions abroad, other than facilities or installations subject to the control of a United States area military commander.

In order to facilitate the fulfillment of these requirements, the Omnibus Act requires other federal agencies to cooperate, to the maximum extent possible, with the Secretary of State through the development of interagency agreements on overseas security. Such agencies may perform security inspections; provide logistical support relating to their differing missions and facilities; and perform other overseas security functions as may be authorized by the Secretary.

II. TERMS OF REFERENCE: (ALPHABETICAL ORDER)

Area Command: A command which is composed of those organized elements of one or more of the armed services, designated to operate in a specific geographical area, which are placed under a single commander; for the purposes of this MOU, the area military commanders are: USCINCEUR; USCINCPAC; USCINCOM; USCINCCENT; and USCINCSO.

Assistant Secretary of State for Diplomatic Security (DS): The office in the Department of State responsible for matters relating to diplomatic security and counterterrorism at U.S. missions abroad.

Consult; Consultation: Refers to the requirement to notify all concerned parties of specific matters of mutual interest prior to taking action on such matters.

Coordinate; Coordination: Refers to the requirement to notify all concerned parties of specific matters of mutual interest and solicit their agreement prior to taking action.

Controlled Access Areas (CAA): Controlled access areas are specifically designated areas within a building where classified information may be handled, stored, discussed, or processed. There are two types of controlled access areas: core and restricted. Core areas are those areas of the building requiring the highest levels of protection where intelligence, cryptographic, security and other particularly sensitive or compartmentalized information may be handled, stored, discussed, or processed. Restricted areas are those areas of the building in which classified information may be handled and stored. Classified discussions are permitted but may be limited to designated areas, depending on the technical security threat.

Defense Components/Defense Component Headquarters: Those DOD organizations which have activities located overseas that fall under the control of the Chief of Mission. Examples include: the Defense Intelligence Agency (DIA) and Defense Security Assistance Agency (DSAA).

Deputy Under Secretary of Defense for Security Policy (DUSD(SP)): The office in the Department of Defense responsible for matters relating to security and counterintelligence [The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C3I) is now the office in DOD responsible for matters relating to security and counterintelligence].

Diplomatic Security Service (DSS) Department of State: The offices of the Department of State responsible for the development, coordination and implementation of security policies and programs domestically and at U.S. missions abroad.

DOD Executive Agent: The Directorate for Security and Counterintelligence, Defense Intelligence Agency (DIA/OSC), has been designated as the office of primary responsibility for DOD, for matters covered by this MOU.

Emergency Action Committee (EAC): An organization established at a Foreign Service post by the Chief of Mission or principal officer, for the purpose of planning and coordinating the post's response to contingencies.

Foreign Service National (FSN): Foreign Service National (FSN) employees are foreign nationals who provide clerical, administrative, technical, fiscal and other support at Foreign Service posts abroad. FSN means an employee of any foreign service-related mission/program/activity of any U.S. Government department or agency overseas establishment including, but not limited to, State, AID, USIA, Commerce, Agriculture, Peace Corps, Department of Defense, (exclusive of consular agents) who is not a citizen of the United States. The term includes Third Country Nationals (TCNs). A TCN is an individual who is employed by a U.S. mission abroad and is neither a citizen of the United States nor of the country to which assigned for duty.

Non-standard Security System: Those items of security equipment which are not in the DS inventory and are not maintainable by DS personnel.

Overseas Security Policy Group (OSPG): The Overseas Security Policy Group develops, coordinates and promotes uniform policies, standards and agreements on overseas security operations, programs and projects which affect U.S. Government civilian agencies represented abroad. The primary functions of the OSPG or subgroups shall be to formulate and develop overseas security policies and guidance for official civilian missions. Implementation of policies adopted by the OSPG or by any agency of the federal government represented at an overseas mission shall be the responsibility of appropriate officials of that agency.

Post Defense Component Office: DOD offices that fall under the control of the Chief of Mission. The following offices, although only a partial listing, are examples: Defense Attache Offices (USDAOs), Joint U.S. Military Aid Groups (JUSMAGs), Joint U.S. Military Assistance Advisory Groups (JUSMAAGs), Joint U.S. Military Missions, U.S. Military Missions (MIIMISH), Military Assistance Advisory Groups (MAAGs), Military Liaison Offices (MLOs), Offices of Defense Cooperation (ODCs), Offices of Defense Representative (ODRs), Offices of Military Cooperation (OMCs), Security Assistance Offices (SAOs), Security Assistance Technical Assistance Field Teams (TAFTs), Select Defense Intelligence Agency Liaison Offices (DIALOs), US Defense Liaison Offices (USDLOs), U.S. Liaison Offices (USLOs), U.S. Military Groups (MILGPs), U.S. Military Training Missions (USMTMs), U.S. Mutual Defense Assistance Office (MDAO).

Regional Security Officer (RSO): The RSO is a U.S. Foreign Service security officer serving abroad at an embassy or consulate who is responsible, through the chain of command to a Chief of Mission, for implementing and managing the Department's overseas security programs. The specific geographical regions for which RSOs have responsibility may include one or more Foreign Service posts.

Sensitive DOD Operational Programs or Activities: Those undertakings by a local Defense Component office which are mandated by DOD, or national-level authorities, and which involve sensitive national defense or national security information or matters. Examples would include: information regarding intelligence activities, sources or methods; national defense plans or contingencies; and special access programs.

Standard Security Equipment and Systems: Security equipment normally in the DS inventory and maintainable by DS personnel.

III. GENERAL ISSUES

A. EXISTING POLICY

Nothing in this agreement shall derogate from or be construed to conflict with the authorities and responsibilities of the Secretary of State, or the Chief of Mission as described in the Omnibus Act (P.L. 99-399), the Foreign Service Act of 1980 (P.L. 96-465) and NSDD-38. The following existing agreements are appended to this MOU and remain in effect between the Departments of State and Defense, to the extent that they do not conflict with this MOU.

1. MOU between the Departments of State and Defense on Utilization and Support of Marine Security Guards. dated December 15, 1986.

2. MOU between the Naval Security and Investigative Command, Department of the Navy, and the Diplomatic Security Service, Department of State relating to the Investigation of Criminal Counterintelligence Matters, dated March 28, 1988.

3. MOU between the Department of State and the Department of the Navy Concerning the Use of Naval Support Unit Personnel Assigned to the Department of State's Security Program, dated December 11, 1978.

4. DOS-DIA Agreement Regarding Support for TEMPEST Personal Computers and Classified-Information Handling Systems, incorporating the DOS-DIA Interagency Control Document (ICD) of July 9, 1984, as amended.

5. STATE AIRGRAM A-41, United States Policy with Regard to Local Guard Forces (LGF) Use by Diplomatic Missions.

B. ISSUES NOT COVERED

Should a particular security issue which is not covered in this MOU develop at a U.S. mission abroad, the interested officials, with the concurrence of the Chief of Mission, will refer the matter to the Department of State and, through the established chain of command, to the DOD Executive Agent for further consideration and subsequent policy guidance.

C. CONFLICTS AT POST

Should a conflict arise at post between the Defense Component office and the RSO concerning the substance or interpretation of this MOU, the interested officials will refer the matter to the Chief of Mission for resolution, through the post Emergency Action Committee (EAC). If further action is required, the post will refer the issue to the Director of the Diplomatic Security Service (DSS) and, through the established chain of command, to the DOD Executive Agent in Washington, DC.

D. EXEMPTIONS

Certain DOD programs, which come under Chief of Mission authority because of their sensitivity (as defined in Section II) shall be exempt, on a case-by-case basis, from the requirements and standards of this MOU. These programs will be separately identified and coordinated in writing between DUSD(SP) and DS.

IV. PHYSICAL, TECHNICAL AND PROCEDURAL SECURITY ISSUES

A. STANDARDS

(1) DS has the responsibility for developing and issuing physical, technical, and procedural security standards, in coordination with the members of the OSPG, and identifying approved security equipment which will enhance the security of all employees of the foreign affairs agencies and all new and existing installations at U.S. missions abroad.

(2) It is the policy of the Department of State to accord security protection on an equitable basis to all U.S. citizen employees of U.S. missions abroad. Any differences in the level of security provided to individuals or categories of employees at post must be based on specific higher threat levels placed on those employees and must be recommended by the post Emergency Action Committee.

(3) With regard to the security afforded to sensitive DOD operational programs and activities, it falls to the local Defense Component office at post to comply with established security program requirements. DOD agrees to comply with DS minimum security standards. If a local Defense Component office requests additional security measures beyond the established minimum level, it will coordinate all requests with the post RSO. If the RSO and the local Defense Component office cannot agree on the level of upgrade requested, they will refer the disagreement, through the Chief of Mission, to the Department of State and, through the established chain of command, the DOD Executive Agent in Washington, D.C. and request resolution of the matter. The additional costs associated with approved security upgrades will be borne by the local Defense Component office through established funding mechanisms. For sensitive DOD operations, the DOD Executive Agent will provide the DS with copies of all applicable DOD component security requirements which exceed DS standards.

(4) Existing physical and technical security standards may be modified, whenever improved deterrents are identified. Physical and technical security equipment will undergo certification testing by U.S. Government agencies and commercial testing laboratories that have been approved by DS. Testing will be done in accordance with DSS-approved test procedures and performance criteria, to ensure that such equipment conforms to established physical security standards.

(5) a. When existing Defense Component office space at post must be relocated, every effort must be made to obtain new space that meets current security standards. If the relocation requires moving to a separate facility outside the post chancery building, every effort will be made to locate a newly constructed facility or an existing building that meets current security standards. If security

standards cannot be met in new space or in a proposed new building, the Chief of Mission and the Defense Component headquarters must be informed and a waiver must be approved by the Assistant Secretary for Diplomatic Security (or designee) before a new facility can be leased or constructed.

b. When the Department of State mandates that post Defense Components be moved to a proposed new facility, yet that facility does not meet all current security requirements, the RSO, working with appropriate DOS offices (e.g., A/FBO), will prepare the required waiver package with input from the Defense Component and submit it formally to the Assistant Secretary for Diplomatic Security-through the Chief of Mission.

c. When the Department of Defense requests that a post Defense Component relocate to a new facility, yet that facility does not meet all current security requirements the DOD Executive Agent will prepare the required waiver package with input from the post Defense Component, the RSO, and other appropriate DOS elements. The waiver package will be submitted to the director of the Diplomatic Security Service, through the Chief of Mission, and according to established waiver procedures. If a waiver is denied, the DOD Executive Agent will have the opportunity to present its case to the Security Exceptions Committee which will evaluate all waiver requests, based on standards contained in the existing DS Physical Security Standards Handbook.

B. SURVEYS CONDUCTED BY SECURITY PERSONNEL NOT RESIDENT AT POST

DS, either on its own (with prior notification to the Chief of Mission and to Defense Component Headquarters through the DOD Executive Agent), or at the request of Defense Component officials, will be responsible for conducting complete physical, technical, and procedural surveys of all Defense Component offices attached to U.S. missions abroad. The security officer conducting the surveys will make recommendations based on standards established in the existing DS Physical Security Standards Handbook and will advise the senior official of the Defense Component office at post, as well as the Chief of Mission, of any weaknesses or deficiencies noted in the course of such surveys. Copies of the survey will be provided to the DOD Executive Agent and DS. DOD will be afforded the opportunity to review and comment on survey recommendations which affect the operations of Defense Component office facilities.

C. SECURITY PROGRAM INSPECTIONS

Representatives of Defense Component Headquarters may conduct periodic or emergency surveys and inspections of their local Defense Component office facil-

ities abroad. Such surveys and inspections may only be conducted with prior notification to the RSO at post through DSS. Further, Defense Component Headquarters and the DOD Executive Agent may review the adequacy of the local guard and residential security services provided to Defense Component offices. On such occasions, the RSO shall make available to Defense Component Headquarters inspectors such information pertaining to Defense Component offices as may be required. Defense Component Headquarters will provide the DSS and the DOD Executive Agent with copies of the final reports of security inspections made by its personnel. If additional resources are required to support DOD's findings, this determination must be referred to both Departments for further coordination. Prior to departure from the post, the Defense Component Headquarters representative conducting the inspection will review the recommendations or issues with the RSO, attempt to resolve them, and provide the RSO with a copy of the draft report. Any remaining differences in recommendations or issues which cannot be resolved at post between the inspecting Defense Component Headquarters representative and the RSO will be handled in accordance with the procedures in Section III-C. of this agreement entitled, "Conflicts at Post."

D. LOCAL GUARD PROGRAM

The RSO shall establish and implement local guard procedures necessary for the security of post Defense Component official facilities and residences. The level of protection provided to the Defense Component office will comply with approved OSPG Local Guard Program standards.

E. RESIDENTIAL SECURITY

The RSO will establish and implement a residential security program applicable to all American personnel under the authority of a Chief of Mission. The level of protection provided to the Defense Component office will comply with approved OSPG Residential Security standards.

F. ARMORED VEHICLES

On a reimbursable basis, Defense Components may arrange with DS to install light vehicle armoring to specifications in local Defense Component office vehicles. The level of protection provided to the Defense Component office will comply with approved OSPG Armored Vehicle standards.

G. FORCED ENTRY/PENETRATION

All instances involving the physical penetration of a building, including unauthorized

entry or damage to property, as well as possible compromise of classified information, will be reported by Defense Component Office personnel to the RSO and the Chief of Mission. The RSO will conduct appropriate investigations and provide the Chief of Mission and the Executive Agent with the full details of the incident, as well as any follow-up action, by telegram via the Department of State. Suspected technical security penetrations and hazards discovered by post Defense Component personnel will be reported to the RSO for appropriate action. Reports of technical security penetrations of or hazards in post Defense Component offices will be provided expeditiously to the DOD Executive Agent by DS, under the provisions of the DCI Procedural Guides I-II-III.

H. STORAGE OF CLASSIFIED MATERIALS

U.S. missions will store and safeguard classified and administratively controlled materials, in accordance with DOS regulations and policies. At facilities approved for storage of classified information, the RSO will designate controlled access areas and establish supervisory controls over the distribution and storage of classified and administratively controlled materials. All Defense Component offices are subject to accreditation by DS for classified storage up to an authorized security classification level, in accordance with DOS Security Standards for the Storage of Classified information at posts abroad.

I. SECURITY VIOLATIONS

The RSO will implement security violation reporting procedures for Defense Component office facilities, in conformance with those specified in existing DOS regulations and policies. All classified material violations involving Defense Component office personnel will be reported directly by the RSO, through mission channels, to the DOD Executive Agent and Defense Component Headquarters for administrative or disciplinary action within thirty (30) days after the violation is discovered. Copies of these reports will also be sent by the RSO to DS.

J. POST TRAINING AND ORIENTATION

The RSO will include U.S. Defense Component office employees at post in training and indoctrination lectures, crisis management drills and in the dissemination of security awareness materials.

K. UNIT SECURITY OFFICERS

Where determined to be of practical operational value and in consultation with the RSO, a Unit Security Officer will be appointed by the Defense Compo-

ment office at post. The Unit Security Officer will be responsible for the conduct of daily physical, technical and procedural security services for the Defense Component office and will assist the RSO, as requested, in DOD investigative activities. The Unit Security Officer will be trained and guided by the RSO in the execution of security functions for post Defense Component offices.

L. REPORTS

Copies of routine reports or correspondence pertaining to all activities conducted by or under the direction of the RSO dealing with the Defense Component office physical, technical, or procedural security matters, will be furnished through mission channels and DS, to the Defense Component Headquarters and DOD Executive Agent. Recommendations for correcting deficiencies as well as corrective action taken will be included in such reports. Alerts, security incidents, or notices of threats to U.S. personnel and facilities under the authority of a Chief of Mission, involving local Defense Component offices or personnel, will be provided to Defense Component Headquarters, the DOD Executive Agent, and the area Commander immediately by telegram. Similarly, Defense Component Headquarters and the DOD Executive Agent will provide copies of correspondence to DS headquarters and RSOs, when communicating on such matters with Defense Component offices at post.

M. INSTALLATION AND MAINTENANCE OF SECURITY SYSTEMS

Subject to survey recommendations, DS will install standard security systems at Defense Component offices at post upon request of the DOD Executive Agent, either by using Security Engineering Officers, Seabees, or Security Engineering Contractors or other cleared American contractors. Equipment installed shall either be procured by DOD Component Offices at post or obtained from the DS inventory. The maintenance of standard DS technical security equipment at Defense Component offices at post will be included in the DS Security Engineering Maintenance Program. The maintenance of non-standard equipment, which is not in DS inventory, will be the responsibility of the post Defense Component office. In cases where Defense Components require technical equipment which is non-standard to the DOS inventory, the local Defense Component office will procure, install and maintain the equipment at its own cost. Non-standard technical equipment will only be used if a DS Security Engineering Officer certifies that it will not interfere with any standard DOS equipment installed. The Defense Component office, with DS concurrence, may contract separately for maintenance of security systems at remote sites which require extensive maintenance of a timely and frequent nature.

N. REQUESTS FOR RSO ASSISTANCE/JOINT INSPECTIONS

Requests from Defense Components Headquarters or the DOD Executive Agent to the RSO for physical, technical and procedural security assistance not addressed elsewhere in this MOU will be cleared through the DS Directorate of Overseas Operations (DS/DSS/OP). In the event of dissatisfaction with security services provided by the RSO to post Defense Components offices and when attempts to resolve problems in consultation with the RSO have failed, the post Defense Component office may bring its concerns to the Chief of Mission, through the Emergency Action Committee (EAC), in accordance with Section III C. of this MOU. The EAC may recommend to the Chief of Mission that a joint inspection of the facilities be performed by the headquarters staff of DS and representatives of the DOD Executive Agent or Defense Component Headquarters, to assess the security services being provided to post Defense Components offices.

O. TECHNICAL SECURITY

DS Security Engineering Officers (SEOs) will include post Defense Component offices in routine technical security countermeasures (TSCM) inspections of controlled access areas at post, where the technical threat warrants such routine inspections. DOD is responsible for the costs of TSCM inspections of Defense Component offices at posts where DS has determined that the technical threat does not warrant more frequent inspections. The Defense Component Headquarters or the DOD Executive Agent may dispatch people and equipment to post to conduct technical security inspections and investigations of post Defense Component Offices. Such activities will be coordinated in advance with DS, the RSO and the DOD Executive Agent. All information obtained from such investigations will be shared with the RSO, the Defense Component Office at post, DS and the DOD Executive Agent and reported to them following the DCI Procedural Guide I-II-III.

P. CONSTRUCTION SECURITY

The Department of State will provide DOD with the construction security training required to enable DOD personnel to perform construction security on non-A/FBO projects in DAO office space within UPS missions abroad. This training will involve construction surveillance techniques and guard responsibilities. Non-A/FBO projects are those which do not substantially change the structural, mechanical, electrical, life-safety, or architectural systems within a U.S. mission abroad.

V. INVESTIGATIONS

A. GENERAL

DS has, inter alia, the responsibility for investigating: a) U.S. citizen applicants, b) foreign national applicants, and c) employees and contractors of DOD at U.S. missions abroad. All requests for investigations, except routine embassy source and police checks originated by the post Defense Component office, will be channeled through DSS to the RSO, or processed as specified in separate agreements. Requests for routine embassy source checks may be made directly to the RSO or Post Security Officer (PSO) by the post Defense Component office. Copies of investigative reports, contact reports and correspondence relating to investigative support of DOD matters or personnel will be furnished to the DOD Executive Agent via DSS. DOD may, at its discretion, dispatch persons from its Defense Component headquarters staff to inquire into a DOD investigative matter. All such activity will be coordinated in advance with the Chief of Mission through the RSO and DS headquarters.

B. U.S. CITIZEN EMPLOYEES, CONTRACTORS AND DEPENDENTS

(1) U.S. citizen employees, contractors and dependents of post Defense Components assigned on a permanent and temporary basis at U.S. missions abroad may be investigated by the RSO: (a) upon the request of the Defense Component headquarters through the DOD Executive Agent and DS; (b) at the direction of the Chief of Mission, when allegations or complaints of a security or suitability nature are received; or, (c) to satisfy USG pre-employment clearance requirements. It is DS policy that RSO's are not authorized to initiate an investigation of a U.S. citizen employee or applicant abroad without the advanced approval of the appropriate DS headquarters element. Should the Chief of Mission direct such an investigation, the RSO may proceed but must immediately notify DS of all relevant information. Prior to initiating an official investigation of any post Defense Component employee or contractor, and subsequent to preliminary inquiries of allegations or complaints, the RSO will report the case to the DOD Executive Agent, via DS, as expeditiously as possible.

(2) No U.S. citizen employee or contractor of DOD, who is the subject of an official investigation by the RSO, shall be interviewed without the approval of and instructions from Defense Component headquarters and the DOD Executive Agent through DS, unless requested by the Chief of Mission. Any time the RSO conducts a formal investigation concerning U.S. citizen employees or contractors

of DOD, a full report shall be forwarded to the Defense Component Headquarters and the DOD Executive Agent via DS. Urgent matters shall be handled by telegram.

(3) Investigations of dependents or proposed dependents of U.S. citizen employees will be conducted consistent with State Department personnel policies, as stated in Volume Three of the Foreign Affairs Manual (3 FAM). Such investigations may be supplemented by DOD, in accordance with established personnel security investigation procedures, when deemed in the interest of national security.

C. FOREIGN NATIONAL EMPLOYEES AND CONTRACTORS

(1) The RSO and the Defense Component office at post will ensure that all foreign nationals proposed for contractual status or employment are investigated, in accordance with established procedures and that the RSO will issue a certification for employment in each approved case. Investigations should be completed prior to employment or execution of a contract. However, such persons may be employed on an interim basis, upon the completion of a satisfactory local investigation and temporary certification by the RSO. Continued employment will be contingent upon satisfactory results of a completed investigation. Foreign National employees and contractors are to be re-investigated and certified every five years.

(2) Allegations of misconduct against foreign national employees and contractors will be investigated by or under the direction of the RSO. Detailed reports of such investigations shall be forwarded to the DOD Executive Agent through DS. The results of such investigations shall be the basis for a determination by the RSO of corrective action to be taken, subject to the concurrence of the Chief of Mission. The RSO will refer to Defense Component Headquarters through DS and the DOD Executive Agent, any cases for which the Chief of Mission believes a decision should be made by Defense Component Headquarters.

(3) The RSO and the Defense Component office at post will ensure that every foreign national, whose position at post requires access to administratively controlled information, is properly investigated and certified.

(4) Security checks and/or investigations of domestic staff of U.S. Defense Component office employees will be conducted consistent with post policy.

VI. TRAINING

A. DS will sponsor DOD Executive Agent personnel for appropriate security-related training offered by the Diplomatic Security Training Center (DS/TC), commensurate with the security clearance level and the need-to-know of the applicant. Such sponsorship is subject to course quota availability.

B. The DOD Executive Agent will sponsor DS personnel for appropriate security-related training, commensurate with the security clearance level and need-to-know of the applicant. Such sponsorship is subject to course quota availability.

VII. BUDGET AND REIMBURSEMENT

A. The Department of State and the Department of Defense will fund diplomatic security programs as specified in the Security Funding Matrix (Appendix A [Appendix E in the Commander's Handbook for Antiterrorism Readiness]) and in accordance with Section IV.A. (2) of this MOU. DOS will fund, within funds available, standard DS security equipment and support that is commensurate with established threat levels. DOD Defense Components will fund, within funds available, non-standard DS security equipment and support which exceeds established threat levels. DOD Defense Component funding will be administered directly between the Defense Component and the Department of State, through contracts that provide security services or support.

B. All DS resource planning will be conducted in consultation with agencies represented at U.S. missions abroad, in order to provide an annual consolidated overseas security budget proposal.

C. Defense Component headquarters, utilizing its authority to protect its personnel and operations under the Internal Security Act of 1950 (50 U.S.C. 797), inter alia, will authorize local Defense Component offices to reimburse the Department of State for security services rendered to local Defense Component offices that exceed DOS funding allocations, upon formal notification of the DOD Executive Agent by DS of the projected security program funding shortfall.

1. Whenever possible, funding shortfalls should be identified in advance of the budget execution year.

2. Reimbursement will be handled through standard procedures for reimbursement for services rendered and will be based upon actual or allocated costs of services rendered to the local Defense Component office under the aegis of the Emergency Action Committee.

VIII. IMPLEMENTATION AND TERMINATION

This Memorandum of Understanding will become effective upon signature by the representatives of the Department of State and the Department of Defense named below. It will remain in force until notification by either party, sixty-days in advance, of its intention to terminate the conditions of the agreement.

/s/ Sheldon J. Krys
U.S. Department of State,
Assistant Secretary for
Diplomatic Security

/s/ Craig Alderman Jr.
U. S. Department of
Defense, Deputy Under
Secretary of Defense
(Security Policy)

APPENDIX D

Security Funding

Delineation of Funding Responsibilities in MOU (Appendix C)

<u>Program:</u>	<u>DOD</u>	<u>DOS</u>
<u>ARMORED VEHICLES (FAV & LAV)</u>		
• Procurement, armoring, and transportation	X	
• Inspection	X	
<u>LOCAL GUARDS (SEE NOTE)</u>		
<u>RESIDENTIAL SECURITY</u>		
• Purchase, install, and maintain residential upgrades		X
<u>PHYSICAL SECURITY, NON-RESIDENTIAL BUILDINGS</u>		
• Purchase, install, and maintain DS standard equipment for nonresidential upgrades		X
• Purchase, install, and maintain nonstandard nonresidential upgrade		X
• Surveys of DOD facilities		X
<u>TECHNICAL SECURITY</u>		
• Purchase, install, and maintain DS standard equipment to meet DS security standards		X
• Purchase, install, and maintain nonstandard equipment or equipment exceeding DS standards	X	
• Maintain equipment at remote DOD sites for which DOS cannot provide timely service	X	
• Surveys of DOD facilities		X
<u>TECHNICAL COUNTERMEASURES</u>		
• Routine TSCM inspections of DOD controlled access areas.		X
• TSCM inspections of DOD-controlled access areas which exceed standard determined by post-threat level		X

Program:**DOD** **DOS****TRANSIT SECURITY**

- Secure shipment, storage, and surveillance of construction materials for FBO projects at DOD controlled access areas X
- Secure shipment, storage, and surveillance of construction materials for non-FBO projects at DOD controlled access areas X
- Secure shipment, storage, and surveillance of non-classified sensitive materials unrelated to construction projects X

CONSTRUCTION SECURITY

- Surveillance and guards for FBO projects at DOD controlled access areas X
- Surveillance and guards for non-FBO projects at DOD-controlled access areas X

TRAINING AND ORIENTATION

- At-post security training specifically requested by DOD and restricted to their personnel only, both US and FSN X
- Washington-based security training offered by DS and DS/TCLGP X

INVESTIGATIONS

- Overseas background investigations (US & FSN) of prospective DOD employees at US missions abroad X
- Investigations of foreign national spouses X

NOTE: Local Defense Component offices are authorized to reimburse DS for the local Defense Component office's share of costs, which exceed the approved field budget plan for a post. LGP costs include roving patrols, static guards and countersurveillance teams where appropriate. Cost share determinations will be based upon the actual or allocated cost of services rendered to the local Defense Component office.

APPENDIX E
Secretary of Defense Memorandum
of 12 December 1995,
Military Assistance to Civil Authorities

(Note: DOD Directive 3025.xx, currently in staffing, will implement the policy outlined below.)

On May 17, 1995, I directed the Under Secretary of Defense for Policy (USD[P]) to establish a working group to review how the Department of Defense provides military assistance to outside agencies. They were charged to examine current procedures, identify deficiencies, and provide recommendations to improve the system. The group reports that our system of providing support is sound but needs modification in some areas, particularly those dealing with emergency responses to natural or man-made disasters or civil disturbances and support to law enforcement.

Approved Criteria. Any request for DOD military support will be evaluated by DOD authorizing authorities against certain fundamental criteria: legality (compliance with laws); lethality (potential use of lethal force by or against DOD forces); risk (safety of DOD forces); cost (who pays, impact on DOD budget); appropriateness (whether the requested mission is in DOD's interest to conduct); and readiness (impact on DOD's ability to perform its primary mission).

Request Procedures. To improve visibility and coordination over outside agency requests, the DOD Executive Secretary will be the principal office charged to keep senior OSD leadership informed of emergency support requests and to be the repository of information on all DOD support to outside agencies. Agencies that receive requests for emergency support may informally coordinate with the requesting agency, but they must immediately notify the Executive Secretary. Outside agencies will be informed that verbal requests for support must be followed by a written request. Non-emergency support requests from federal agency headquarters will be in writing. The Executive Secretary will establish notification procedures within 60 days of this memorandum and advise me as to necessary changes and staff expansion.

Approval Authority - Execution Procedures.

Emergency Support. When DOD responds to acts of terrorism whether overseas or domestically, I will personally oversee such matters. For such responses, the CJCS will assist me to operationally manage these crises using the Joint Staff, assisted in domestic incidents by the Army's Director of Military Support (DOMS) in managing the consequences of a terrorist incident (WMD, Oklahoma City, etc.). The USD(P) and the CJCS, in coordination with the DOD GC, will ensure that our policies and operational procedures are consistent and comply with applicable federal laws and Presidential directives, whether responding to traditional terrorist incidents or ones dealing with weapons of mass destruction (nuclear, chemical, or biological).

All emergency support to civil disturbances (MACDIS) because they may lead to the use of lethal force, will be approved by me. In particular, I will approve the rules of engagement for our forces in responding to a civil disturbance. For emergency support to a natural or man-made disaster (MSCA), support approval is delegated to the SECARMY, unless a CINC's assets are involved. In such MSCA actions, the DOMS staff will develop the courses of action for submission with the request through the Joint Staff to the Chairman prior to obtaining my decision. Following my decision, the CJCS will transmit orders through DOMS to the appropriate CINC for execution and management by the SECARMY. When CINC assets are not involved, the SECARMY, as my Executive Agent, may task the Services or DOD agencies directly to provide emergency support.

The Executive Agent (SECARMY) will retain his dedicated staff, currently established under the Director of Military Support (DOMS), to respond to domestic emergency support requests. The CJCS will assist the SECARMY in ensuring that the DOMS staff has adequate Joint Staff expertise by identifying select full time positions as joint critical and pre-designating Joint Staff members to augment DOMS during a crisis.

As an example, an outside agency, such as the FBI/DOJ (civil disturbance emergencies) or FEMA (emergency disasters), seeking assistance in a domestic emergency, will go to the DOMS staff, who will notify the Executive Secretary and Joint Staff of the request and begin staffing the action. For a civil disturbance emergency, because of its potential for use of lethal force, the DOMS staff will always forward the support request with recommended courses of action through the Joint Staff and Chairman to me for a decision. For FEMA requests dealing with emergency disasters, the DOMS staff will review the request to determine if the request can be handled by a Service's assets alone or if CINC assets are required.

If the former is the case, the DOMS staff will submit the request with recommended courses of action to the SECARMY for approval and subsequent tasking of the appropriate Service(s). In the event that a CINC's assets are required to deal with an emergency disaster, the DOMS staff will submit the support request with recommended courses of action through the Joint Staff and the CJCS to me for a decision. Following my decision, in either a civil disturbance emergency or emergency disaster requiring CINC assets, the Chairman will send the order through DOMS to the appropriate CINC for execution and management by the Secretary of the Army.

Non-Emergency Support. Overall, our non-emergency support system is satisfactory. Procedural and approval authorities for sensitive support to outside agencies will remain as presently constituted and comply, as necessary, with the guidelines defined below. Requests for support from civilian law enforcement agencies must be carefully examined prior to approval. No request will be approved without a legal review. Such requests must be approved or under oversight by a general officer or senior civilian equivalent. All law enforcement requests must be evaluated against the intended purpose of the support. Any requests to assist law enforcement agencies that will result in a planned event with the potential for confrontation with named individuals/groups or use of lethal force must be forwarded to my office for approval.

Overall. Any support provided by my Executive Agent in emergency matters, or by Service Secretaries for non-emergency matters, that impacts on readiness, must be brought to the attention of the CJCS. As part of revised reporting procedures, I want the Executive Secretary to be notified of any engineer support provided by the Services to outside agencies pursuant to the Stafford Act or other legislative authority that is not covered by other emergency support reporting means.

Implementation. The USD(P) will lead an effort to identify for information, revision, or cancellation those DOD directives, memorandums of understanding/agreement (MOU/MOA), policies, CONPLANS, and regulations, which impact on military assistance to outside agencies. In particular, clear definitions should be developed for MOUs/MOAs and procedures delineated on how the Executive Secretary's office can maintain for my review all MOUs/MOAs agreed to by DOD. The working group will oversee the updating of directives, regulations, etc. to ensure they meet the intent of this memorandum. The USD(P) will provide me periodic updates and a final report no later than six months from today. Supporting CONPLANS will be updated or established by the CJCS within eight months from the date of this memorandum.

I applaud the efforts of the work done to date. I expect the same thoroughness and cooperation in completing this very important undertaking for DOD and the many outside agencies we support. Our goal is to streamline our procedures and ensure accountability, without degrading our responsiveness to the needs of the nation.

/s/ William J. Perry
Secretary of Defense

APPENDIX F

References

EXECUTIVE / INTERAGENCY

Presidential Decision Directive 39, “US Policy on Counterterrorism.”

“Public Report of the Vice President’s Task Force on Combating Terrorism,” February 1986.

Memorandum of Understanding Between the Department of State and the Department of Defense, 22 January 1992.

Memorandum of Understanding Between the Department of Defense, the Department of Justice, and the Federal Bureau of Investigation, 5 August 1983.

LEGISLATIVE

Title 10 - US Code, Armed Forces.

Title 18 - US Code, Sections, Crimes and Criminal Procedure.

Title 21 - US Code, Food and Drugs.

Title 33 - US Code, Navigation and Navigable Waters.

Title 42 - US Code, Public Health and Welfare.

Title 49, - US Code, Transportation.

Public Law 98-473, Omnibus Diplomatic Security and Antiterrorism Act of 1986.

DEFENSE

“Force Protection Assessment of USCENTCOM AOR and Khobar Towers: Report of the Downing Assessment Task Force,” 30 August 1996.

“Report to the President: The Protection of U.S. Forces Abroad,” Submitted by the Secretary of Defense, 16 September 1996.

Secretary of Defense Memorandum, “Military Assistance to Civil Authorities,” 22 January 1992.

DOD Directive 2000.12, “DOD Combating Terrorism Program,” Revised and Reissued 15 September 1996.

DOD Handbook 2000.12 -H. “Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence,” February 1993.

DOD Instruction 2000.14, “DOD Combating Terrorism Program Procedures,” 15 June 1994.

DOD Directive 3025.1, “Military Support to Civil Authorities” (MSCA).

DOD Directive 3025.12, “Military Assistance for Civil Disturbances” (MACDIS).

DOD Directive 3025.xx (Draft), “Military Assistance to Civil Authorities.”

DOD Directive C-4500.51, “DOD Non-Tactical Armored Vehicle Policy.”

DOD Directive 5200.8, “Security of Military Installations and Resources.”

DOD Directive 5200.8-R, “Physical Security Program.”

DOD Instruction 5210.84, “Security of DOD Personnel at US Missions Abroad.”

DOD Directive 5240.10, DOD “Counterintelligence Support to Unified and Specified Commands.”

DOD Directive 5525.5, “DOD Cooperation with Civilian Law Enforcement Officials.”

JOINT STAFF

Joint Vision 2010, Special Publication

Joint Pub 1-02, “DOD Dictionary of Military and Associated Terms.”:

Joint Pub 2-0, “Joint Doctrine for Intelligence Support to Operations.”

Joint Pub 3-07.2, “Joint Tactics, Techniques, and Procedures for Antiterrorism.”

Joint Pub 3-10, “Doctrine for Joint Rear Area Operations.”

Joint Pub 3- 11, “Joint Doctrine for Nuclear, Biological, and Chemical (NBC) Defense.”

Joint Pub 3-54, “Joint Doctrine for Operations Security.”

Joint Pub 3-58, "Joint Doctrine for Military Deception."

Joint Staff Guide 5260, "Service Member's Personal Protection Guide: A Self-Help Handbook to Combating Terrorism," July 1996.

Joint Staff Pamphlet 5260 [Family/Individual], "Coping With Violence: Personal Protection Pamphlet," July 1996.

CJCSM 3500.03, "Joint Training Manual for the Armed Forces of the United States."

CJCSM 3500.04A, "Universal Joint Task List."

RELATED INTERNET SITES (As of October 1996)

Citizen Militias:

http://www.tcac.com/~steveb/cit_mil.html

Emergency Response Research Institute (ERRI) Terrorism and Counter-Terrorism Home Page:

<http://www.emergency.com/cntrterr.html>

ERRI Terrorist Leaders:

<http://www.emergency.com/Terr-Ldr.htm>

Milnet: Terrorism:

<http://www.onestep.com:80/milnet/terror.htm>

Rand Corporation Subject Index to Terrorism:

<http://www.rand.org/areas/TERC.Toc.html>

Terrorist Profile Weekly

<http://www.site.gmu.edu/~cdibona>

Van Impe Intelligence Briefing

<http://www.niagara.com/~jvim/IntelligenceBriefing>

Worldwide Acts of Terrorism

<http://www.onestep.com/milnet/terrchrn.htm>

ADDITIONAL READING

Alexander, Yonah. Middle East Terrorism: Selected Group Profiles.

Washington, Jewish Institute for National Security Affairs, 1994.

Anderson, Sean and Sloan, Stephen. Historical Dictionary of Terrorism.

Metuchen, NJ, Scarecrow Press, 1995.

Atkins, Stephen E. Terrorism: A Reference Handbook. Santa Barbara, CA

ABC-CLIO, 1992.

Bodansky, Yossef. Target America & the West: Terrorism Today. New York,

S.P.I. Books/Shapolsky Publishers, 1993.

Clutterbuck, Richard. Terrorism in an Unstable World. New York,

Routledge, 1994.

European Terrorism: Today & Tomorrow, edited by Yonah Alexander and

Dennis A. Pluchinsky. New York, Brassey's (US) Inc. 1992.

Haugfht, James A. Holy Hatred: Religious Conflicts of the '90s. Amherst,

New York, 1995.

Patterns of Global Terrorism: 1995. Washington, US Dept. of State.

Shafritz, Jay M. and others. Almanac of Modern Terrorism. New York,

Facts on File, 1991.

Smith, Brent L. Terrorism in America: Pipe Bombs and Pipe Dreams.

Albany, State University of New York Press, 1994.

Terrorism: National Security Policy and the Home Front, edited by Stephen

C. Pelletiere, US Army War College Strategic Studies Institute, 1995.

White, Jonathan R. Terrorism: An Introduction. Pacific Grove, CA,

Brooks-Cole Publishing, 1991.

for further reading see:

Terrorist and Insurgent Organizations, Air University Special Bibliography

No. 301 compiled by Janet L. Seymour, June 1996.

GLOSSARY

PART I—Abbreviations and Acronyms

ACIC	Army Counterintelligence Center
AFOSI	Air Force Office of Special Investigations
AOR	area of responsibility
AT	antiterrorism
ATCC	Antiterrorism Coordinating Committee
C3I	command, control, communications and intelligence
CCB	Community Counterterrorism Board
CIA	Central Intelligence Agency
CID	Criminal Investigation Command
CINC	commander of a combatant command
CJCS	Chairman of the Joint Chiefs of Staff
CJCSM	Chairman, Joint Chiefs of Staff Manual
COM	Chief of Mission
CONUS	continental United States
CT	counterterrorism
DEFCON	Defense Readiness Condition
DIA	Defense Intelligence Agency
DIWS	Defense Indications and Warning System
DLO	Defense Liaison Office
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction

DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
DS	Assistant Secretary of State for Diplomatic Security
DSAA	Defense Security Assistance Agency
DSS	Diplomatic Security Service
EAC	Emergency Action Committee
EI	essential elements of information
ELINT	electronics intelligence
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSN	foreign service national
GC	Geneva Convention
HQMC (CIC)	Headquarters, US Marine Corps, Counterintelligence/ HUMINT Branch
HUMINT	human intelligence
IAW	in accordance with
ICD	Interagency Control Document
IDS	intrusion detection system
IED	improvised explosive device
IG	Inspector General
J-2	Director of Intelligence, The Joint Staff
J-34	Deputy Director for Operations (Combating Terrorism), The Joint Staff

JCS	Joint Chiefs of Staff
JTF	joint task force
JUSMAAG	Joint US Military Assistance Advisory Group
JUSMAG	Joint US Military Advisory Group
MDAO	US Mutual Defense Assistance Office
MILGP	US Military Groups
MLO	military liaison offices
MOU	memorandum of understanding
MOA	memorandum of agreement
NAVATAC	Navy Antiterrorism Alert Center
NMCC	National Military Command Center
NSC	National Security Council
NSD	National Security Directive
NSDD	National Security Decision Directive
OASD (PA)	Office of the Assistant Secretary of Defense (Public Affairs)
OASD (SO/LIC)	Office of the Assistant Secretary of Defense (Special Operations/ Low Intensity Conflict)
OCONUS	outside of the continental United States
ODC	Office of Defense Cooperation
ODR	Office of Defense Representative
OMC	Office of Military Cooperation
OPSEC	operations security
OSD	Office of the Secretary of Defense
OSINT	open-source intelligence
OSPG	overseas security policy group

PAO	public affairs officer
POM	Program Objective Memorandum
PDD	Presidential Decision Directive
RAM	random antiterrorism measures
ROE	rules of engagement
RSO	Regional Security Officer
SAO	Security Assistance Office
SECDEF	The Secretary of Defense
SIGINT	signal intelligence
SJA	staff judge advocate
SOFA	Status-of-Forces Agreement
TAFT	security assistance technical assistance field team
TCN	third country nationals
THREATCON	terrorist threat condition
TWR	Defense Terrorism Warning Report
USACIDC	United States Army Criminal Investigation Command
USAJFKSWCS	United States Army J.F. Kennedy Special Warfare Center and School
USAMPS	United States Army Military Police School
USCINCOM	Commander in Chief, US Atlantic Command
USCINCEUR	Commander in Chief, US European Command
USCINCCENT	Commander in Chief, US Central Command
USCINCPAC	Commander in Chief, US Pacific Command
USCINCSO	Commander in Chief, US Southern Command

USCINCSOC	Commander in Chief, US Special Operations Command
USCINCSPACE	Commander in Chief, US Space Command
USCINCSTRAT	Commander in Chief, US Strategic Command
USCINCTRANS	Commander in Chief, US Transportation Command
USD(P)	Under Secretary of Defense for Policy
USDAO	US Defense Attache Office
USIA	US Information Agency
USLO	US Liaison Office
USMTM	US Military Training Mission
WMD	weapons of mass destruction

GLOSSARY

PART II—Definitions

- A antiterrorism**—Defensive measures used to reduce the vulnerability of individuals and property to terrorism, to include limited response and containment by local military forces. Also called **AT**.
- C combating terrorism**—Actions, including antiterrorism taken to oppose terrorism throughout the entire threat spectrum.
- counterterrorism**—Offensive measures taken to prevent, deter, and respond to terrorism. Also called **CT**.
- crisis management force**—An installation’s assets capable of reacting to an incident.
- D deterrence**—The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.
- F force protection**—Security program designed designed to protect soldiers, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs.
- H high-risk personnel**—Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets.
- hostage**—A person held as a pledge that certain terms or agreements will be kept. (The taking of hostages is forbidden under the Geneva Convention 1949.)
- I initial response force**—The first unit, usually military police, on the scene of a terrorist incident.
- installation**—A grouping of facilities, located in the same vicinity, that support particular functions. Installations may be elements of a base.
- installation commander**—The individual responsible for all base operations.

insurgency—An organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict.

insurgent—Member of a political party who rebels against established leadership.

N National Command Authorities—The President and the Secretary of Defense or their duly deputized alternates [or successors]. Also called NCA.

negotiations—Discussions between authorities and a barricaded offender/terrorist to effect hostage release and terrorist surrender.

O open source intelligence—Information of potential intelligence value that is available to the general public. Also called OSINT.

operations security—A process of analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence

b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC.

P physical security—That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft.

prevention—The security procedures undertaken by the public and private sector in order to discourage terrorist acts.

primary targets—An object of high publicity value to terrorists.

proactive measures—Measures taken in the preventive stage of antiterrorism designed to harden targets and detect actions before they occur.

R revolutionary—An individual attempting to effect a social or political change through the use of extreme measures.

S sabotage An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources.

secondary targets—Alternative targets of lower publicity value. Attacked when primary target is unattainable.

security—1. Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness. 2. A condition that results from the establishment and maintenance of proactive measures that ensure a state of inviolability from hostile acts or influences.

status-of-forces agreement—An agreement which defines the legal position of a visiting military force deployed in the territory of a friendly state. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement, or they form part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or its members to the local law or to the authority of local officials.

T terrorism—The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

terrorist—An individual who uses violence, terror, and intimidation to achieve a result.

terrorist groups—Any element regardless of size or espoused cause, which repeatedly commits acts of violence or threatens violence in pursuit of its political, religious, or ideological objectives.

threat analysis—A continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups which could target a facility. A threat analysis will review the factors of a terrorist group's existence, capability, intentions, history, and targeting, as well as the security environment within which the friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment.

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

FOR OFFICIAL USE ONLY



FOR OFFICIAL USE ONLY